CICS

Supporting Individuals. Strengthening Communities.

Regional Governing Board

June 23, 2022 @ 1:00PM

Hertz Farm Management

415 S 11th Street, Nevada, Iowa 50201

SPECIAL NOTE TO THE PUBLIC: Members of the public who would like to call in: 1-312-626-6799
Meeting ID: 872 3015 6219, Passcode: 107617
or Join the Zoom Meeting at https://us06web.zoom.us/j/87230156219?pwd=czVpZU9mUzJhTno1Z1A4MWxKdHo5dz09

Tentative Agenda

1) Roll Call

☐ Boone	☐ Cerro Gordo	☐ Franklin	☐ Greene
☐ Hamilton	☐ Hancock	☐ Hardin	☐ Jasper
☐ Madison	☐ Marshall	☐ Poweshiek	☐ Story
☐ Warren	☐ Webster	☐ Wright	☐ JD Deambra
☐ Allie Wulfekuhle	☐ Kendra Alexander	☐ Julie Smith	☐ Andrea Dickerson

2) Agenda (BJ Hoffman, Chair)

June 23, 2022 Agenda **Action**

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

3) Minutes (BJ Hoffman, Chair)

May 26, 2022 Minutes **Action**

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

4) Administration (Karla Webb, Operations Officer)

ICAP (Property Insurance Update and Liability Insurance Renewal) **Action**

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

Fiscal Agent Agreement **Action**

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

Memorandums of Understanding between CICS and Franklin County **Action**

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

ISAC HIPAA Program Service Agreement **Action**

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

HIPAA Policies and Procedures **Action**

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

HIPAA Emergency Mode Operations Plan **Action**

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

Business Associate Agreements between CICS and the following counties: **Action**

Franklin County

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

Hardin County

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

Story County

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

Out of Pocket Reimbursement Update **Informational**

5) Finance (Karla Webb)

May Expenditure Report **Informational**

Claims May 31 and June 14, 2022 **Action**

Board Chair asks for motion to approve.

Motion by: _____

Second: _____

Vote on motion: _____

Roll call vote (mark if 'aye')

☐ Boone	☐ Cerro Gordo	☐ Franklin	☐ Greene
☐ Hamilton	☐ Hancock	☐ Hardin	☐ Jasper
☐ Madison	☐ Marshall	☐ Poweshiek	☐ Story
☐ Warren	☐ Webster	☐ Wright	☐ JD Deambra
☐ Allie Wulfekuhle	☐ Kendra Alexander		

6) Operations (Karla Webb)

FY22 Contract – Pillar of Cedar Valley **Action**

Board Chair asks for motion to approve/deny

Motion by: _____

Second: _____

Vote on motion: _____

Abstaining: _____

FY23 IRSH Contract with North Iowa Transitional Services Inc. dba 43 North Iowa **Action**

Board Chair asks for motion to approve/deny

Motion by: _____

Second: _____

Vote on motion: _____

Abstaining: _____

FY23 Contracts **Action**

Arc of Marshall County
Boone County Mental Health Advocate Agreement
Capstone Behavioral Healthcare
Center Associates
Central Iowa Juvenile Detention Center
Central Iowa Psychological Services
Cerro Gordo County Mental Health Advocate Agreement
Choices Therapy Services, LLC
Eyerly Ball Community Mental Health Services
Hamilton County Mental Health Advocate Agreement
Hardin County Mental Health Advocate Agreement
Jasper County Mental Health Advocate MOU
Judicial Hospital Referee Agreement
Liberty Square dba Spring Harbor Residential Services
Mason City Clinic

Orchard Place
Pillar of Cedar Valley
Region 6 Resource Partners
Rodasi LLC dba Midwest Counseling
Youth Shelter Care of North Central Iowa, Inc.

Board Chair asks for motion to approve/deny
Motion by: _____
Second: _____
Vote on motion: _____
Abstaining: _____

7) Public Comments
Board Chair asks for public comments at this time

8) Next Meeting – July 28, 2022

Regional Governing Board Meeting Minutes
May 26, 2022
Hertz Farm Management, Nevada, IA

Board Members Present: Boone, Cerro Gordo, Franklin, Greene, Hancock, Hardin, Jasper, Madison, Marshall, Poweshiek, Story, Warren, Webster, Andrea Dickerson, JD Deambra, Kendra Alexander. **Counties/Members Absent:** Hamilton, Wright, Allie Wulfekuhle, Julie Smith. **Administrative Team Present:** Russell Wood, Linn Adams, Patti Leeds, Betsy Stursma, Karla Webb. **OthersPresent:** Thomas Laehn, Greene County Attorney.

Agenda & Minutes
Motion to approve the May 26, 2022 agenda. Motion by Talsma, second by Watts. All ayes, motion carried.

Motion to approve the April 28, 2022 minutes. Motion by Talsma, second by Dawley. All ayes, motion carried.

Russell Wood, CEO discussed the hybrid model for Information Technology and requested to repost the position at the step 5 minimum salary. **Motion by Watts, second by Hoffman to approve reposting the IT position at the step 5 minimum salary as presented. All ayes, motion carried.**

Dawn Rudolph introduced Thomas Laehn, Greene County Attorney. Laehn explained he reviewed the 28E by suggestion of the Board of Supervisors. There are two conflicting statements on how a county may be added in the 28E. Laehn also would like the fiscal year defined in the 28E agreement to avoid ambiguity. Hoffman asked for questions or comments from the Board. Hoffman stated it is clear that there is a conflict in the 28E agreement, however it can't be acted on today. This can be on next month's agenda if needed. Wood stated DHS would have to approve any changes to the 28E agreement. Hoffman asked if Laehn would collaborate with the CICS attorney to clear up the language. Laehn has proposed language to fix the issues. He asked for clarification on how the Governing Board decides. Wood stated that it is unanimous consent to add a county. Stursma stated it is a 2-step process. The first is to have the new county come to the Board to request being added to the CICS region and step two is to take it to the individual counties before approving. Wood stated the fiscal year is in Iowa Code, but can be added in. Hoffman appreciates the attorney did his due diligence and does not have an issue with the collaboration to amend the 28E. Heddens asked if Wood would be involved, so the intent of the Board is not changed. Wood suggested the chair or vice-chair are part of the collaboration and also he is not sure that it will get back to the Board by June. Wood stated if they wait until July much of the language can be removed due to Iowa Code. A strikethrough agreement would be presented to the Board after the collaboration and review by the admin team and DHS agree on it. Nolte asked for clarification on if it was to be unanimous or majority vote. Wood stated it needs to be unanimous. If a county wants to join they come to the Board, which requires a majority vote, then it goes to the counties and comes back to the GB for a unanimous vote to approve the new county.

Finance Officer Betsy Stursma shared the claims report for May 3 and 17, 2022. **Motion by Heddens, second by Talsma to approve claims. All ayes, motion carried on roll call vote. Stursma also provided the April expenditure report.**

Stursma brought the Board up-to-date on Fund 10. As of July 2, Fund 10 will no longer exist. She has reached out to all county auditors for their end of April fund balance and projections for May and June. In mid-June an initial check will be sent to the fiscal agent with the bulk of Fund 10. At the end of June 30 auditors are asked to do a handwritten check to the fiscal agent to close out the remaining balance.

Stursma is continuing to work with counties on occupancy in county controlled buildings. June 15 is the cutoff for agreements for occupancy to be able to be paid on the last claims run. Wood commented that a lot of lease agreements state on or before July 1. There is one county remaining for agreements to occupancy. If there are any county IT departments that need CICS to make changes, the administrative team would request that they reach out quickly. Wood clarified that some counties will allow CICS to stay on the county network and some counties will not. CICS just needs to know what needs to be done.

Planning and Development Officer Patti Leeds stated there was one proposal received for IRSH for a 4-bedroom IRSH home, meeting all requirements needed for an IRSH. They are currently enrolled with Medicaid. There is a property in Mason City that would be remodeled and they are asking for the remodeling costs of the home to be able to provide IRSH at that location. They have agreed to work with CICS to contribute to the outcome measurements for the region. December is their projection to be up and running. The budget was less than what was expected. Wood stated the action made today would be to instruct Admin to work with 43 North Iowa to move forward with the proposal. The final action would be in June for deciding whether to approve the final contract. Access fees were discussed. IRSH has a cap on what Medicaid will fund. The region pays the difference if it is over the cap. There has been discussion that the actual cost for IRSH will be higher than the cap. If so, legislation would have to increase the cap in the future if it needs to be changed. CICS will only pay an access fee if it is above the cap. **Motion by Watts, seconded by DeKock to instruct CICS staff to negotiate with 43 North Iowa**. Kretzinger wanted clarification on the utilization of the facility. Is this only for CICS clients, or is this for any region to use. Wood stated that it may be possible to put in the contract if the Board would like it to be only for CICS clients. Wood stated if someone moves in from another county they would be gaining residency in CICS anyway. Clifton asked for information regarding upkeep of the home. Leeds stated it is a house they already own, upkeep would have to be discussed with 43 North Iowa. Watts was questioning the ability to expand in the future. Wood stated IRSH can only be 5 beds max and this location is proposed as a 4-bed. **All ayes, motion carried.**

Hoffman spoke with a law enforcement officer recently about trainings. Hoffman asked if sending those recommendations to Leeds was the proper procedure. Leeds is fine with that and in the future that will be appropriate also. Hoffman asked if CICS backfills if reserve officers are needed to cover shifts. Wood stated mileage, meals, lodging and reserves for shift coverage if needed. Hoffman encouraged the Board to bring suggestions if they run across anything that would fit for CICS to train on, etc.

Operations Officer Karla Webb presented the contract with explained the onboarding cost and the monthly cost of the Heartland Business Systems (HBS) IT contract. There is a help desk option for staff to be able to reach out to. They require devices to be updated within 3 years (NOTE THAT SINCE THE MEETING HBS HAS CLARIFIED THAT 5 YEARS WOULD BE ACCEPTABLE), some devices may need to be replaced. Franklin County IT looked at the agreement and had no concerns about the contract. Heddens asked if there is

a rotation for upgrading systems. Wood explained it depends on the county as to what previously was purchased. Wood explained the domain will be on the cloud rather than on the Franklin County domain. It will be different as everyone will be completely removed form their current network. Legacy data does need to be on the cloud, if not already moved. There will be no access on CICS equipment to any county servers. All CICS data will be on the CICS domain. There will be HIPAA business associates agreements that will need to be signed. Kretzinger asked how HBS was decided on. Wood stated RFPs were sent out and HBS came in with the better proposal. HBS is a Wisconsin company, however they have a local Des Moines office. **Motion by Kretzinger, seconded by Rudolph to approve contract as presented with Heartland Business Systems. All ayes, motion carried**.

Webb presented the FY22 contract for Norse Ventures, LLC, dba Thrive. **Motion by Clifton, seconded by Rayhons to approve the FY22 contract for Norse Ventures, LLC, dba Thrive. All ayes, motion carried.**

Webb presented the FY23 contract for HIRTA. **Motion by Talsma, seconded by Dawley to approve the FY23 contract with HIRTA. All ayes, motion carried. Clifton and Heddens abstained.**

Webb presented FY23 contracts for Brian Vold, ARNP; Integrated Behavioral Health Services, P.C. dba Classroom Clinic; Community & Family Resources; Crossroads Mental Health Center; Foundation 2, Inc.; Greene County Medical Center dba Greene County Family Medicine; eVizzit of Iowa Psychiatric PC Integrated Telehealth Partners; North Central Sheltered Workshop dba LifeWorks Community Services; Lutheran Services in Iowa; Mainstream Living; Mary Greeley Medical Center; New Beginnings Counseling Services; Norse Ventures LLC., dba Thrive; Optimae Life Services; Plains Area Mental Health, Inc.; Premier Payee, Inc.; Progress Industries; and Salvation Army. **Motion by Campbell, seconded by Deambra to approve FY23 contracts as presented. All ayes, motion carried.**

Board Chair asked for public comment. Heddens asked for clarification of whether Green County has signed the current 28E agreement. It was stated that Greene County did sign the current 28E. Wood stated he and Stursma would not be at the June meeting and Webb would fill the role for admin team lead.

Next Meeting is **June 23, 2022**.

Chair adjourned the meeting.

_____ _____

Patti Leeds, Recording Secretary BJ Hoffman, Board Chair

Iowa Communities Assurance Pool

INVOICE

FOR

Central Iowa Community Services

Anniversary Date: 07/01/2022

12951 University Ave, Ste 120
Clive, IA 50325
www.icapiowa.com

Iowa Communities Assurance Pool

Member Invoice

Member Name: Central Iowa Community Services

Policy Number: R0891PC2022-2

Anniversary Date: 07/01/2022

Coverage	Limit of Coverage	Contribution
General Liability	$2,000,000	$10,424
Auto Liability	$2,000,000	$91
Public Officials Liability	$2,000,000	$3,665
Excess Liability	$0	$0
TOTAL CONTRIBUTION		**$14,180**

MAKE CHECKS PAYABLE TO IOWA COMMUNITIES ASSURANCE POOL ON OR BEFORE:
07/01/2022

Payment for this invoice can be submitted electronically via the ICAP website. Please visit www.icapiowa.com and click "Member Pay" at the top right of the page to pay via ACH transfer. There is no fee for utilizing this service. If you require assistance or prefer to pay via check, please contact the ICAP office via 1-(800) 383-0116.

Iowa Communities Assurance Pool

Member Proxy

Be it known, that the undersigned representative of the Governmental Sub-Division (hereafter referred to as MEMBER) by resolution of the governing body, a copy of which is attached hereto, hereby nominates and appoints the following individual and alternate to represent the MEMBER with the Iowa Communities Assurance Pool (hereinafter referred to as the POOL). The individual and alternate shall act as liaison between MEMBER and the POOL for the purposes of relating risk reduction and loss control information, and any other loss information or instructions concerning the obligations of the MEMBER imposed by signing the Iowa Risk Management Agreement and the rules and regulations established thereunder, to the same extent and with like effect as the undersigned thereunder, to the same extent as the undersigned could do if personally present and the undersigned does hereby ratify and confirm and adopt all action done or taken by the individual or alternate.

Primary Contact:	Russell Wood	Alternate Contact:	BJ Hoffman
Title:	Regional CEO	Title:	Chair
Address:	126 S. Kellogg Ave., Ste. 001	Address:	Hardin County Courthouse
Address:		Address:	1215 Edgington Ave.
City, State, Zip:	Ames, IA 50010	City, State, Zip:	Eldora, IA 50627
Email:	Russell.Wood@cicsmhds.org	Email:	bhoffmah@hardincountyia.gov
Telephone:	515-663-2928	Telephone:	641-939-8220

In witness whereof, this proxy was executed on the_____day of_____, in the year _____, by the undersigned duly authorized officers of the Governmental Subdivision indicated below:

Governmental Subdivision: Central Iowa Community Services

Member ICAP #: 0891

By: _____

Title: _____

By: _____

(City Clerk/County Auditor/Board Secretary)

Iowa Communities Assurance Pool

Anniversary Information Acknowledgement

The undersigned representative of the Central Iowa Community Services acknowledges that he/she:

- ☐ Reviewed the information provided on all Iowa Communities Assurance Pool applications and all applicable supplemental applications.
- ☐ Reviewed all applicable property and vehicle schedules.
- ☐ Confirms, to the best of his/her knowledge, that all information provided is complete and accurate.
- ☐ Reviewed the optional coverage(s) offered by the Iowa Communities Assurance Pool for increased limits. After consideration of the coverage(s) offered and the contribution for same, Central Iowa Community Services has elected to:
  - ☐ Waive any and all coverage(s) and any applicable contribution charges. Central Iowa Community Services understands that to add increased limits coverage in the future, it will be subject to Iowa Communities Assurance Pool's approval and underwriting guidelines at the time of the request and that such request must be made in writing. In addition, Central Iowa Community Services will not hold the Iowa Communities Assurance Pool responsible for this decision to waive optional coverage(s).
  - ☐ Accept the increased limits: _____ (Limit of Liability Accepted)

Executed on the _____ day of _____ , in the year _____ , by the undersigned duly authorized officer of the Governmental Subdivision Central Iowa Community Services indicated below:

By: _____

Title: _____

Member: Central Iowa Community Services
Member Number: 0891
Anniversary Date: 07/01/2022

Iowa Communities Assurance Pool

Quote Summary

Central Iowa Community Services

Anniversary Date: 07/01/2022

Coverage	Contribution	Limit of Coverage	Deductible	Retroactive Date	Coverage Effective
General Liability	$10,424	$2,000,000	$0	07/01/2022	7/1/2022
Auto Liability	$91	$2,000,000	$0	07/01/2022	7/1/2022
Public Officials Liability	$3,665	$2,000,000	$3,000	07/01/2022	7/1/2022
Excess Liability	$0	$0		07/01/2022	7/1/2022
TOTAL CONTRIBUTION	**$14,180**				
FINAL CONTRIBUTION	**$14,180**				

Excess Liability Options	Contribution	Limit of Liability	Coverage Effective
Excess Liability	$1,499	$1,000,000	07/01/2022
Excess Liability	$2,741	$2,000,000	07/01/2022
Excess Liability	$3,891	$3,000,000	07/01/2022
Excess Liability	$4,996	$4,000,000	07/01/2022
Excess Liability	$6,052	$5,000,000	07/01/2022
Excess Liability	$7,065	$6,000,000	07/01/2022
Excess Liability	$8,029	$7,000,000	07/01/2022
Excess Liability	$8,948	$8,000,000	07/01/2022
Excess Liability	$9,820	$9,000,000	07/01/2022
Excess Liability	$10,647	$10,000,000	07/01/2022
Excess Liability	$11,425	$11,000,000	07/01/2022
Excess Liability	$12,163	$12,000,000	07/01/2022
Excess Liability	$12,879	$13,000,000	07/01/2022

Payment for this invoice can be submitted electronically via the ICAP website. Please visit www.icapiowa.com and click "Member Pay" at the top right of the page to pay via ACH transfer. There is no fee for utilizing this service. If you require assistance or prefer to pay via check, please contact the ICAP office via 1-(800) 383-0116.

This quotation expires on the Proposed Effective Date.

Iowa Communities Assurance Pool

Commitment to Continue Membership

I, Central Iowa Community Services, do hereby affix my signature to this form and promise to submit the contribution of $14,180.00 (less attached vouchers if applicable) by _____. In order to fulfill this commitment, our payment will be received by the Iowa Communities Assurance Pool, at the address on this form, no later than _____.

Printed Name _____

Signature _____

Date _____

Iowa Communities Assurance Pool
12951 University Ave, Ste 120
Clive, IA 50325

Iowa Communities Assurance Pool

General Liability Breakout

Central Iowa Community Services

Anniversary: 7/1/2022

	Total Contribution	% of Total
Net Operating Expenditures	$10,424	100.00 %
Total	$10,424	
Public Officials Wrongful Acts	$3,665	
Total	$3,665	

Iowa Communities Assurance Pool

Auto Liability Breakout

Central Iowa Community Services

Anniversary: 7/1/2022

Hired Non-Owned	$91
Total	$91

FISCAL AGENT AGREEMENT
Effective July 1, 2022

This agreement, effective the 1st day of July, 2022, is between Central Iowa Community Services, hereafter referred to as CICS, and Story County, hereafter referred to as the Fiscal Agent.

I. **Purpose of Agreement**

CICS has been formed under *Code of Iowa* Chapter 28E and wishes to add efficiencies in financial management through the consolidation of accounting practices of its member counties and further wishes to designate a public entity as a fiscal agent to administer its funds. Story County has been designated as said Fiscal Agent.

II. **Duration of Agreement**

This agreement shall be effective July 1, 2022, and shall remain in effect until June 30, 2025, or until earlier terminated according to the provisions herein. This agreement may be amended, renewed, or extended by the mutual written agreement of the parties in the form of an amendment specifying the new agreement period and the compensation to the Fiscal Agent. All other terms of the agreement shall remain in effect unless otherwise specifically amended.

III. **Responsibilities of the Fiscal Agent**

The Fiscal Agent shall provide the following services:

A. Deposit CICS funds into the MHOS CICS Regional Fiscal Agency Fund, hereafter referred to as Fund 41500, in accordance with *Code of Iowa* Chapter 12C and provide copy of bank statement monthly after reconciled by the Treasurer of Fiscal Agent County.
B. Issue payments from Fund 41500 as directed by authorized CICS personnel. Payments shall be issued to the individual, vendor, business, or other entity identified by CICS, in the amount specified, and to the address provided by CICS. Payments shall be issued as directed, within seven (7) workdays from the date the Fiscal Agent receives the approved claim with supporting documentation from authorized CICS personnel.
C. Ensure that any interest earned on Fund 41500 shall be credited directly to Fund 41500.
D. Direct bank fees shall be charged directly to Fund 41500 and shall not be considered a part of the Fiscal Agent compensation as outlined in *Section VI. Compensation of this Agreement.*
E. All other approved expenses including the annual audit (that portion of costs as identified by the Auditor of State, State of Iowa) will be submitted to the CICS finance officer for a claim to be processed.
F. Be responsible for completing and submitting any 1099 reports as required by federal or state law or regulation.
G. Maintain separate accounting records as requested that at a minimum include the following:
    1. Utilize the integration between Fiscal Agent's financial software (Solutions) and the Community Services Network (CSN}.
    2. Submit to finance officer the disbursement register for claims paid.
    3. Quarterly Fund 41500 Outstanding Report.
    4. The date of any stop payment requested by the Fiscal Agent and reason.
H. Submit to the CICS finance officer monthly Fund Balance, Revenue and Expense detail and summary reports for the prior month by the 15th of the month. Reports shall be submitted in a format agreed to by CICS and Fiscal Agent and shall include as much of the information

as the Fiscal Agent is required to maintain as described in this section as CICS may request and as is necessary to reconcile the records of CICS with the records of the Fiscal Agent.

I. Resolve any findings outlined in the annual completed audit by working with necessary parties including, but not limited to, CICS and Finance Committee.

J. If this agreement is renewed or extended any unexpended CICS funds remaining in an account held by the Fiscal Agent at the end of the current agreement period shall be retained by the Fiscal Agent for use in the next agreement period.

K. If this agreement is not renewed or extended, unexpended CICS funds, and accrued interest as may be required by law, shall be transferred to the new fiscal agent.

L. Submit a report to CICS of any audits performed as well as the findings of any audits of the accounting records for the Fiscal Agent. The report shall be submitted to CICS within five (5) work days of its receipt by the Fiscal Agent.

M. The Fiscal Agent shall chair the CICS Finance Committee.

IV. Responsibilities of CICS

A. Advise the Fiscal Agent in writing of the identity of CICS personnel authorized to approve and submit payment request from CICS funds to the Fiscal Agent and to receive and review expenditure and other reports from the Fiscal Agent as required herein.

B. Determine the amount and payee for any payment to be made from CICS funds.

C. Authorized personnel shall submit a dated written authorization to the Fiscal Agent to make payments from CICS funds.

D. Maintain accounting records for CICS payments authorized to be paid by the Fiscal Agent that, at a minimum, includes the following:

1. Date written notification/authorization was submitted to the Fiscal Agent.
2. Name of the authorized CICS personnel authorizing the payment.
3. Name and mailing address of the payee.
4. Amount of the payment.
5. General Ledger account code for payment.

E. Review on a monthly basis the monthly expenditure reports submitted by the Fiscal Agent and reconcile with the records maintained by CICS. CICS and Fiscal Agent shall work together to resolve any discrepancies and take any necessary corrective action.

V. General Provisions

A. *Agreement Amendment*. The agreement shall be amended only upon written approval of both parties.

B. *Renegotiation Clause*. In the event there is a revision of federal regulations, state laws, or administrative rules and this agreement no longer conforms to those regulations, laws, or rules, all parties will review the agreement and renegotiate those items necessary to conform with the new regulations, laws, or rules.

C. Termination of Agreement

1. *For Cause.* Causes for termination during the period of agreement are:
   a. Failure of Fiscal Agent to complete or submit required reports.
   b. Failure of Fiscal Agent to make financial and statistical records available for review by CICS or other authorized party.
   c. Failure of Fiscal Agent to abide by the terms of this agreement.
   d. Failure of CICS to abide by the terms of this agreement.

➢ If any of (a) through (c) above occurs, CICS shall provide written notice to Fiscal Agent requesting that the noncompliance be remedied immediately. In the event

that the noncompliance continues fifteen (15) days beyond the date of the Fiscal Agent's receipt of written notice, CICS may either immediately terminate the agreement without additional notice or enforce the terms and conditions of the agreement and seek any legal or equitable remedies.

- If (d) above occurs, the Fiscal Agent shall provide written notice to the Chief Executive Officer of CICS, hereafter referred to as CEO, requesting that the noncompliance be remedied immediately. In the event that the noncompliance continues fifteen (15) days beyond the date of the CEO receipt of written notice, Fiscal Agent may either immediately terminate the agreement without additional notice or enforce the terms of the agreement and seek legal or equitable remedies.

2. *Upon notice*. Either party may terminate this agreement by providing 180 days written notice to the other party.

D. *Confidentiality*. Fiscal Agent shall comply with the Health Insurance Portability and Accountability Act (HIPAA) and all applicable federal and state laws and regulations on confidentiality.

E. *Federal and State Compliance*. Fiscal Agent shall be in compliance with all applicable federal and state laws, rules, and regulations.

F. *Records Retention*. Fiscal Agent shall maintain records that document the validly of reports submitted to CICS. The fiscal Agent shall retain all books, records, electronic records or other documents relevant to this agreement for a period of two (2) years after this agreement is no longer in effect or after the final completed audit has been submitted, whichever is later.

G. *Review of Contract Related Documentation*. Fiscal Agent shall allow authorized representatives of CICS or state or federal agencies to have access to the records as is necessary to confirm compliance with the specifications of this agreement. Reviews may include on-site visits to the Fiscal Agent, the offices of the Fiscal Agent's agents, a combination of these, or, by mutual decision, to other locations.

VI. **Compensation**

A. Compensation for the Fiscal Agent shall be $1,200 per month until otherwise amended.

B. The Fiscal Agent shall submit at least a quarterly invoice to CICS for payment.

C. CICS shall pay the cost of the audit associated with the regional fund 41500.

SIGNATURE PAGE

By: _____

BJ Hoffman, Chairperson
Central Iowa Community Services

Date

By: _____

Patti Treibel-Leeds, Recording Secretary
Central Iowa Community Services

Date

By: _____ 5.24.22

Latifah Faisal, Chairperson
Story County Board of Supervisors

Date

By: _____ 5.24.22

Lucy Martin, Auditor
Story County

Date

By: _____ 5-24-22

Ted Rasmusson, Treasurer
Story County

Date

Supporting Individuals. Strengthening Communities.

MEMORANDUM OF UNDERSTANDING (MOU) between
Franklin County, Iowa
and
Central Iowa Community Services (CICS)

This is an agreement between Franklin County, Iowa, hereinafter referred to as "Franklin County" and Central Iowa Community Services, hereinafter referred to as "CICS."

I. PURPOSE and SCOPE

The purpose of this MOU as identified in the 28E Agreement between Franklin County, Iowa and Central Iowa Community Services Section 1.1 is "Franklin County and CICS shall have a Memorandum of Understanding (MOU) for each employee performing duties for CICS, and such MOU will identify full time equivalent (FTE) status, rate of pay, and years of service (for initial employees the MOU will include number of hours of paid leave the employee will have upon transfer to Franklin County)."

II. EMPLOYEE DETAILS

NAME	FTE STATUS	RATE of PAY	CALCULATED HIRE DATE	YEARS of SERVICE

PAID LEAVE*	
VACATION	SICK LEAVE

*Paid leave balances identified are from the current employing county's first pay period in June for this employee. Updated employee paid leave details will be provided to Franklin County by CICS in an additional document as soon as the information is available after 7/1/22 from the county the employee is transferring to Franklin County from.

III. EFFECTIVE DATE AND SIGNATURE

This MOU shall be effective 7/1/22 – 6/30/23, or upon employee changes.

Signature and Dates:

_____ _____
Gary McVicker, Franklin County, Iowa Board Chair BJ Hoffman, CICS Governing Board Chair

_____ _____
Date Date

CICS and Franklin County Employee MOU Detail

Employee							Paid Leave	
Last Name	First Name	FTE Status	Rate of Pay		Calculated Hire Date	Years of Service	Vacation	Sick Leave
McKee	Robin	100%	$70,532.80	Annually	9/17/2007	14	133.55	900.00
Wood	Russell	100%	$107,120.00	Annually	3/17/2003	19	313.84	900.00
Sheehan	Jen	100%	$27.84	Hourly	7/1/2013	9	136.50	235.00
Crawford	Jessica	100%	$25.23	Hourly	6/7/2017	5	80.08	251.29
Freie	Meghan	100%	$29.02	Hourly	4/11/2011	11	116.10	515.10
Hill	Lisa	100%	$22.20	Hourly	1/25/2016	6	96.24	215.39
Baker	Brittany	100%	$26.77	Hourly	7/1/2014	8	89.25	253.50
Martinson	Tanya	100%	$22.32	Hourly	7/1/2013	9	163.50	206.50
Leanhart	Lisa	100%	$22.08	Hourly	7/1/2015	7	51.50	265.75
Varrelmann	Starla	100%	$23.78	Hourly	7/1/2020	2	42.00	115.00
Sprecher	Nicole	100%	$27.30	Hourly	10/22/2012	9	72.68	432.54
Johnson	Kathy	100%	$27.84	Hourly	1/20/1998	24	164.70	568.08
Lennon	Tyler	100%	$24.87	Hourly	3/19/2018	4	64.70	347.65
Radley	Jennifer	100%	$18.77	Hourly	2/22/2022	0	22.33	37.67
Webb	Karla	100%	$99,840.00	Annually	3/23/1998	24	197.10	900.00
Adams	Linn	100%	$99,840.00	Annually	1/2/1985	37	212.77	715.50
Hamilton	Jodi	90%	$27.84	Hourly	9/28/2010	11	55.10	32.89
Hisler	Carrie	100%	$32.05	Hourly	6/24/1996	26	209.74	900.00
Lauchner	Michelle	75%	$19.05	Hourly	4/1/2020	2	0	0
Treibel Leeds	Patti	100%	$99,840.00	Annually	10/5/2005	16	132.75	751.85
White	Jarica	100%	$25.23	Hourly	11/14/2016	5	78.74	569.30
Christensen	Christy	90%	$27.93	Hourly	5/22/2019	3	80.00	40.00
Gerke	Kelly	100%	$20.22	Hourly	8/16/2016	5	25.70	360.00
Soder	Lisa	100%	$27.84	Hourly	3/11/2002	20	171.19	360.00
Daily	Brenda	100%	$29.89	Hourly	1/27/2016	6	68.75	900.00
Howard	Liza	100%	$64,376.00	Annually	6/20/2016	6	79.97	65.24
Stursma	Elizabeth	95%	$101,920.00	Annually	7/1/2005	17	320.00	407.55
Van De Voort	Jess	100%	$27.62	Hourly	5/31/2016	6	14.03	3.76
Schomaker	Kim	100%	$28.82	Hourly	11/7/2005	16	320.00	268.20

This Memorandum of Understanding (hereinafter "MOU") is entered into between Central Iowa Community Services (CICS) and Boone County, Iowa.

I. **MENTAL HEALTH DISABILITY SERVICES CLIENT FILES.** In recognition that Boone
II. County, Iowa is a member county of Central Iowa Community Services 28E Agreement to create a mental health and disability service region to provide local access to mental health and disability services, it is acknowledged that ownership and possession of client mental health and disability services files generated prior to July 1, 2013 shall be transferred to CICS effective July 1, 2022. The following special responsibilities are assumed by the parties:

a. **CICS Responsibilities.** CICS agrees to:
    i. Follow and implement Health Insurance Portability and Accountability Act (HIPAA) requirements
    ii. Follow and implement any other Federal, State, or local laws governing confidentiality of client information

b. **Boone County Responsibilities.** Boone County agrees to:
    i. Release client files to CICS
    ii. Inform individuals requesting records to contact CICS

III. **TERMINATION.** This MOU shall remain in effect through June 30, 2023. The requirements under I. a. and I. b. shall survive the ending or termination of this agreement. The agreement is subject to revision due to legislation, change in operating practices and policies of the involved parties, or other factors, as agreed to by the involved parties. It may be amended by mutual written agreement of the parties.

IV. **INDEMNIFICATION**. Each party agrees to hold harmless all other parties (including its officers, agents and employees) from and against any and all claims, demands, liabilities and costs incurred by the indemnified party, including reasonable attorney's fees, directly or indirectly arising out of or in connection with the indemnifying party's performance, or any service, or any other act or omission by or under the direction of the indemnifying party, or its officers, agents or employees.

V. **NOTICES.** All notices related to this MOU shall be addressed as follows:

a. To: Boone County Board of Supervisors:
   Attn: Board Chair Steve Duffy
   201 State Street
   Boone Iowa 50036

b. To: CICS – Story County
   Attn: Operations Officer
   126 S. Kellogg Ave., Ste. 001
   Ames, IA 50010

IN WITNESS WHEREOF, the parties have here unto set their hand, and the effective date of this agreement is the _____day of _____2022 .

Boone County BOARD OF SUPERVISORS
201 State Street
Boone Iowa 50036

By:_____
Chair, Boone County Board of Supervisors

Date: _____

CENTRAL IOWA COMMUNITY SERVICES
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010

By: _____
Chair, CICS Governing Board

Date: _____

This Memorandum of Understanding (hereinafter "MOU") is entered into between Central Iowa Community Services (CICS) and Greene County, Iowa.

I. **MENTAL HEALTH DISABILITY SERVICES CLIENT FILES.** In recognition that Greene
II. County, Iowa is a member county of Central Iowa Community Services 28E Agreement to create a mental health and disability service region to provide local access to mental health and disability services, it is acknowledged that ownership and possession of client mental health and disability services files generated prior to July 1, 2013 shall be transferred to CICS effective July 1, 2022. The following special responsibilities are assumed by the parties:

a. **CICS Responsibilities.** CICS agrees to:
   i. Follow and implement Health Insurance Portability and Accountability Act (HIPAA) requirements
   ii. Follow and implement any other Federal, State, or local laws governing confidentiality of client information

b. **Greene County Responsibilities.** Greene County agrees to:
   i. Release client files to CICS
   ii. Inform individuals requesting records to contact CICS

III. **TERMINATION.** This MOU shall remain in effect through June 30, 2023. The requirements under I. a. and I. b. shall survive the ending or termination of this agreement. The agreement is subject to revision due to legislation, change in operating practices and policies of the involved parties, or other factors, as agreed to by the involved parties. It may be amended by mutual written agreement of the parties.

IV. **INDEMNIFICATION.** Each party agrees to hold harmless all other parties (including its officers, agents and employees) from and against any and all claims, demands, liabilities and costs incurred by the indemnified party, including reasonable attorney's fees, directly or indirectly arising out of or in connection with the indemnifying party's performance, or any service, or any other act or omission by or under the direction of the indemnifying party, or its officers, agents or employees.

V. **NOTICES.** All notices related to this MOU shall be addressed as follows:

a. To: Greene County Board of Supervisors:
   Attn: Board Chair John Muir
   114 N. Chestnut Street
   Jefferson Iowa 50129

b. To: CICS – Story County
   Attn: Operations Officer
   126 S. Kellogg Ave., Ste. 001
   Ames, IA 50010

IN WITNESS WHEREOF, the parties have here unto set their hand, and the effective date of this agreement is the _____day of _____2022 .

Greene County BOARD OF SUPERVISORS
114 N. Chestnut Street
Jefferson Iowa 50129

By: _____
Chair, Greene County Board of Supervisors

Date: 6/13/2022

CENTRAL IOWA COMMUNITY SERVICES
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010

By: _____
Chair, CICS Governing Board

Date: _____

This Memorandum of Understanding (hereinafter "MOU") is entered into between Central Iowa Community Services (CICS) and Hamilton County, Iowa.

I. **MENTAL HEALTH DISABILITY SERVICES CLIENT FILES.** In recognition that Hamilton
II. County, Iowa is a member county of Central Iowa Community Services 28E Agreement to create a mental health and disability service region to provide local access to mental health and disability services, it is acknowledged that ownership and possession of client mental health and disability services files generated prior to July 1, 2013 shall be transferred to CICS effective July 1, 2022. The following special responsibilities are assumed by the parties:

a. **CICS Responsibilities.** CICS agrees to:
   i. Follow and implement Health Insurance Portability and Accountability Act (HIPAA) requirements
   ii. Follow and implement any other Federal, State, or local laws governing confidentiality of client information

b. **Hamilton County Responsibilities.** Hamilton County agrees to:
   i. Release client files to CICS
   ii. Inform individuals requesting records to contact CICS

III. **TERMINATION.** This MOU shall remain in effect through June 30, 2023. The requirements under I. a. and I. b. shall survive the ending or termination of this agreement. The agreement is subject to revision due to legislation, change in operating practices and policies of the involved parties, or other factors, as agreed to by the involved parties. It may be amended by mutual written agreement of the parties.

IV. **INDEMNIFICATION.** Each party agrees to hold harmless all other parties (including its officers, agents and employees) from and against any and all claims, demands, liabilities and costs incurred by the indemnified party, including reasonable attorney's fees, directly or indirectly arising out of or in connection with the indemnifying party's performance, or any service, or any other act or omission by or under the direction of the indemnifying party, or its officers, agents or employees.

V. **NOTICES.** All notices related to this MOU shall be addressed as follows:

a. To: Hamilton County Board of Supervisors:
   Attn: Board Chair Rick Young
   2300 Superior Street
   Webster City Iowa 50595

b. To: CICS – Story County
   Attn: Operations Officer
   126 S. Kellogg Ave., Ste. 001
   Ames, IA 50010

IN WITNESS WHEREOF, the parties have here unto set their hand, and the effective date of this agreement is the _____day of _____2022 .

Hamilton County BOARD OF SUPERVISORS
2300 Superior Street
Webster City Iowa 50595

By:_____
Chair, Hamilton County Board of Supervisors

Date: 6/14/22

CENTRAL IOWA COMMUNITY SERVICES
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010

By: _____
Chair, CICS Governing Board

Date: _____

This Memorandum of Understanding (hereinafter "MOU") is entered into between Central Iowa Community Services (CICS) and Hardin County, Iowa.

I. **MENTAL HEALTH DISABILITY SERVICES CLIENT FILES.** In recognition that Hardin County, Iowa is a member county of Central Iowa Community Services 28E Agreement to create a mental health and disability service region to provide local access to mental health and disability services, it is acknowledged that ownership and possession of client mental health and disability services files generated prior to July 1, 2013 shall be transferred to CICS effective July 1, 2022. The following special responsibilities are assumed by the parties:

a. **CICS Responsibilities.** CICS agrees to:
   i. Follow and implement Health Insurance Portability and Accountability Act (HIPAA) requirements
   ii. Follow and implement any other Federal, State, or local laws governing confidentiality of client information

b. **Hardin County Responsibilities.** Hardin County agrees to:
   i. Release client files to CICS
   ii. Inform individuals requesting records to contact CICS

II. **TERMINATION.** This MOU shall remain in effect through June 30, 2023. The requirements under I. a. and I. b. shall survive the ending or termination of this agreement. The agreement is subject to revision due to legislation, change in operating practices and policies of the involved parties, or other factors, as agreed to by the involved parties. It may be amended by mutual written agreement of the parties.

III. **INDEMNIFICATION**. Each party agrees to hold harmless all other parties (including its officers, agents and employees) from and against any and all claims, demands, liabilities and costs incurred by the indemnified party, including reasonable attorney's fees, directly or indirectly arising out of or in connection with the indemnifying party's performance, or any service, or any other act or omission by or under the direction of the indemnifying party, or its officers, agents or employees.

IV. **NOTICES.** All notices related to this MOU shall be addressed as follows:

a. To: Hardin County Board of Supervisors:
   Attn: Board Chair
   1215 Edgington Ave., Ste. 1
   Eldora, IA 50627

b. To: CICS – Story County
   Attn: Operations Officer
   126 S. Kellogg Ave., Ste. 001
   Ames, IA 50010

IN WITNESS WHEREOF, the parties have here unto set their hand, and the effective date of this agreement is the _____day of _____2022 .

HARDIN COUNTY BOARD OF SUPERVISORS
1215 Edgington Ave. Ste. 1
Eldora, IA 50627

By:_____
Chair, Hardin County Board of Supervisors

Date: _____

CENTRAL IOWA COMMUNITY SERVICES
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010

By: _____
Chair, CICS Governing Board

Date: _____

MOU Between Central Iowa Community Services and Marshall County, Iowa

This Memorandum of Understanding (hereinafter "MOU") is entered into between Central Iowa Community Services (CICS) and Marshall County, Iowa.

I. **MENTAL HEALTH DISABILITY SERVICES CLIENT FILES.** In recognition that Marshall County, Iowa is a member county of Central Iowa Community Services 28E Agreement to create a mental health and disability service region to provide local access to mental health and disability services, it is acknowledged that ownership and possession of client mental health and disability services files generated prior to July 1, 2013, shall be transferred to CICS effective July 1, 2022. The following special responsibilities are assumed by the parties:

a. **CICS Responsibilities.** CICS agrees to:
   i. Follow and implement Health Insurance Portability and Accountability Act (HIPAA) requirements
   ii. Follow and implement any other Federal, State, or local laws governing confidentiality of client information

b. **Marshall County Responsibilities.** Marshall County agrees to:
   i. Release client files to CICS
   ii. Inform individuals requesting records to contact CICS

II. **TERMINATION.** This MOU shall remain in effect through June 30, 2023. The requirements under I. a. and I. b. shall survive the ending or termination of this agreement. The agreement is subject to revision due to legislation, change in operating practices and policies of the involved parties, or other factors, as agreed to by the involved parties. It may be amended by mutual written agreement of the parties.

III. **INDEMNIFICATION.** Each party agrees to hold harmless all other parties (including its officers, agents and employees) from and against any and all claims, demands, liabilities and costs incurred by the indemnified party, including reasonable attorney's fees, directly or indirectly arising out of or in connection with the indemnifying party's performance, or any service, or any other act or omission by or under the direction of the indemnifying party, or its officers, agents or employees.

IV. **NOTICES.** All notices related to this MOU shall be addressed as follows:

a. To: **Marshall County Board of Supervisors**
   Attn: Board Chair
   1 East Main Street
   Marshalltown, IA 50158

b. To: **CICS – Story County**
   Attn: Operations Officer
   126 S. Kellogg Ave., Ste. 001
   Ames, IA 50010

IN WITNESS WHEREOF, the parties have here unto set their hand, and the effective date of this agreement, **MOU Between Central Iowa Community Services and Marshall County, Iowa,** is the 1st day of July, 2022.

MARSHALL COUNTY
BOARD OF SUPERVISORS
1 East Main Street
Marshalltown, IA 50158

By: _____
Dave Thompson, Chair
Marshall County Board of Supervisors

Date: _____

Attestation: _____

By: _____
Nan Benson
Marshall County Auditor and Recorder

Marshall County Seal:

CENTRAL IOWA COMMUNITY SERVICES
126 S Kellogg Ave., Ste. 001
Ames, IA 50010

_____
B.J. Hoffman, Chair
CICS Governing Board

Date: _____

Attestation or Notary: _____

By: _____

Attestation or Notary

State of Iowa
County of _____
Signed and sworn to (or affirmed) before me on

_____ (date), by **B.J. Hoffman**
to me personally known, or has produced identification, as Chair, on behalf of **CICS Governing Board**
(Type of ID)_____

_____
Signature of Notary Public
My commission expires: _____
(seal)

This Memorandum of Understanding (hereinafter "MOU") is entered into between Central Iowa Community Services (CICS) and Story County, Iowa.

I. **MENTAL HEALTH DISABILITY SERVICES CLIENT FILES.** In recognition that Story County, Iowa is a member county of Central Iowa Community Services 28E Agreement to create a mental health and disability service region to provide local access to mental health and disability services, it is acknowledged that ownership and possession of client mental health and disability services files generated prior to July 1, 2013 shall be transferred to CICS effective July 1, 2022. The following special responsibilities are assumed by the parties:

a. **CICS Responsibilities.** CICS agrees to:
   i. Follow and implement Health Insurance Portability and Accountability Act (HIPAA) requirements
   ii. Follow and implement any other Federal, State, or local laws governing confidentiality of client information

b. **Story County Responsibilities.** Story County agrees to:
   i. Release client files to CICS
   ii. Inform individuals requesting records to contact CICS

II. **TERMINATION.** This MOU shall remain in effect through June 30, 2023. The requirements under I. a. and I. b. shall survive the ending or termination of this agreement. The agreement is subject to revision due to legislation, change in operating practices and policies of the involved parties, or other factors, as agreed to by the involved parties. It may be amended by mutual written agreement of the parties.

III. **INDEMNIFICATION.** Each party agrees to hold harmless all other parties (including its officers, agents and employees) from and against any and all claims, demands, liabilities and costs incurred by the indemnified party, including reasonable attorney's fees, directly or indirectly arising out of or in connection with the indemnifying party's performance, or any service, or any other act or omission by or under the direction of the indemnifying party, or its officers, agents or employees.

IV. **NOTICES.** All notices related to this MOU shall be addressed as follows:

a. To: Story Co. Board of Supervisors:
   Attn: Board Chair
   Story County Administration Building
   900 6th Street, Nevada, IA 50201

b. To: CICS – Story County
   Attn: Operations Officer
   126 S. Kellogg Ave., Ste. 001
   Ames, IA 50010

MOU Between Central Iowa Community Services and Story County, Iowa

IN WITNESS WHEREOF, the parties have here unto set their hand, and the effective date of this agreement is the _____day of _____2022 .

STORY COUNTY BOARD OF SUPERVISORS
900 6th Street
Nevada, IA 50201

By: _____
VICE Chair, Story County Board of Supervisors

Date: 6-14-22

CENTRAL IOWA COMMUNITY SERVICES
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010

By: _____
Chair, CICS Governing Board

Date: _____

ISAC HIPAA Program

What's included?

- Annual sixty minute "HIPAA 101" training via webinar for employees in your county or MHDS region.
- One of the following annual training options available only to participating counties or MHDS regions and designed for your HIPAA security/privacy officers, HIPAA committee members or other staff that work with HIPAA and PHI regularly. The training option will be decided based on a combination of speaker availability and preference of ISAC HIPAA Program members.
    - One day long (approximately 10 a.m. to 3 p.m.) in-person training in Des Moines for up to 5 persons from your county or MHDS region.
    - Multi-day (approximately 3, 60-minute webinars) virtual training with no limit on member attendance.
- Access to all memos and other information previously generated through the ISAC HIPAA Program via an ISAC HIPAA Program member website.
- Access to all memos and other information generated through all member consultation hour questions as a part of the current year of the ISAC HIPAA Program via an ISAC HIPAA Program member website.
- Up to 5 hours annually for consultation on HIPAA questions. All participating counties and MHDS regions will be required to select a HIPAA contact for purposes of the program. All questions shall come from this contact and be directed to Beth Manley, ISAC Compliance Officer. Beth will collect all questions and prepare responses or submit them to Alissa Smith, partner with the Dorsey & Whitney law firm. An estimate of the time needed to answer a question will be provided prior to beginning research. All legal research memos created in response to questions will be disseminated to all ISAC HIPAA Program participants via the ISAC HIPAA Program member website.
- If the program member has questions that exceed their consultation hours, the additional time will be billed to the program member. An estimate of the time needed to answer a question will be provided prior to beginning the research.
- If consultation hours are not used, the dollars will be invested in additional trainings and educational resources for the ISAC HIPAA Program.
- Quarterly newsletter, received via e-mail, with HIPAA news, reminders, checklists and other updates.
- Webinar series about various HIPAA topics. Past topics have included information on risk assessments, staff training, cyber security, and other relevant topics. If needed, a MHDS region webinar will be included in the webinar series.
- Online training platform with access to various HIPAA courses.

What is the cost to a county or a MHDS region?

New County: $1,950

New Region: $2,000

Returning County or Region Participant: $1,750

Who should participate?

Any county or MHDS region that would like basic consultation, assistance and training on general HIPAA topics and issues.

When does the ISAC HIPAA Program start?

The ninth year of the program will run from July 1, 2022 to June 30, 2023.

How do we sign up?

Have your county or MHDS Region approve and execute the "Service Agreement to Participate in the ISAC HIPAA Program" and return it to ISAC. Returning counties and MHDS Region participants must sign a new Service Agreement.

Other questions?

Please contact Beth Manley at (515) 244-7181 or bmanley@iowacounties.org.

SERVICE AGREEMENT TO PARTICIPATE IN THE ISAC HIPAA PROGRAM

This Service Agreement to Participate in the ISAC HIPAA Program (the "Agreement"), effective as of July 1, 2022 (the "Effective Date") is hereby entered into by and amongst Central Iowa Community Services (CICS) (known as the "Region") and the Iowa State Association of Counties ("ISAC") (collectively referred to as the "Parties") to set forth the terms and conditions under which the Region will become a participant in the ISAC HIPAA Program (the "HIPAA Program").

For the consideration as described below, the Parties agree as follows:

Description of HIPAA Program

The following services will be provided to all participants in the HIPAA Program:

1. Annual sixty minute "HIPAA 101" training via webinar for employees in your county or MHDS region.
2. One of the following annual training options available only to participating counties or MHDS regions and designed for your HIPAA security/privacy officers, HIPAA committee members or other staff that work with HIPAA and PHI regularly. The training option will be decided based on a combination of speaker availability and preference of ISAC HIPAA Program members.
    - One day long (approximately 10 a.m. to 3 p.m.) in-person training in Des Moines for up to 5 persons from your county or MHDS region.
    - Multi-day (approximately 3, 60-minute webinars) virtual training with no limit on member attendance.
3. Access to all memos and other information previously generated through the ISAC HIPAA Program via an ISAC HIPAA Program member website.
4. Access to all memos and other information generated through all member consultation hour questions as a part of the current year of the ISAC HIPAA Program via an ISAC HIPAA Program member website.
5. Up to 5 hours annually for consultation on HIPAA questions.
6. Quarterly newsletter, received via e-mail, with HIPAA news, reminders, checklists and other updates.
7. Webinar series about various topics. If needed, a MHDS region webinar will be included in the webinar series.
8. Online training platform with access to various HIPAA courses.

In exchange for these services and administration of the services, the Region will pay ISAC an annual fee of $1,750.

Region Responsibilities

1. Execute this Agreement.
2. Pay the annual fee of $1,750 by the Effective Date. This fee is non-refundable and no portion of the fee shall be returned to the Region in the event the Region opts not to participate in a training or does not utilize all of its consultation hours.
3. Select a HIPAA contact person for purposes of the HIPAA Program as set forth below.

4. Direct all HIPAA questions through the HIPAA contact person to ISAC Compliance Officer. ISAC shall be the client of Dorsey and Whitney for purposes of the HIPAA program and all communications with Dorsey and Whitney shall be through ISAC or with ISAC's permission. Failure to comply with this provision may result in the Region being billed outside of the HIPAA Program at Alissa Smith's regular rate.
5. The HIPAA contact person will promptly respond to inquiries from ISAC Compliance Officer related to HIPAA questions.

ISAC Responsibilities

1. Retain Alissa Smith, partner with the Dorsey and Whitney law firm, to provide trainings and consultation for the HIPAA program.
2. Oversee HIPAA questions and disseminate consultation on HIPAA questions ISAC Compliance Officer will collect all questions and prepare responses or submit them to Alissa Smith, partner with the Dorsey & Whitney law firm. An estimate of the time needed to answer a question will be provided prior to Alissa Smith beginning. All legal research memos created in response to questions will be disseminated to all ISAC HIPAA Program participants via the ISAC HIPAA Program member website.
3. If the program member has questions that exceed their consultation hours, the additional time will be billed to the program member. An estimate of the time needed to answer a question will be provided prior to beginning the research.
4. Track the consultation hours used by the Region in the HIPAA Program.
5. Coordinate and staff the HIPAA trainings of the HIPAA Program.

Term

The term of this agreement shall be from the Effective Date of this Agreement to June 30, 2023.

Mutual Responsibilities

The Parties agree to indemnify and hold each other harmless for any and all costs, including attorney's fees and cost of collection, that may reasonably result from such Party's failure to comply with the terms and conditions of this Agreement, its intentional or negligent act or omission related to this Agreement, or for any breach of the provisions of this Agreement. Liability of the parties for any damages sustained as a result of breach of this Agreement, or arising in any way out of this Agreement, shall be limited to actual damages.

The Region understands that participation in the ISAC HIPAA Program in no way guarantees compliance with HIPAA and that ISAC is not assuming any liability or responsibility for the Region's HIPAA compliance and that all such liability and responsibility remains that of the Region.

Amendments of this Agreement shall be made by mutual consent of the Parties, by issuance of a written amendment, signed and dated by all Parties.

This Agreement constitutes the entire agreement between the Parties concerning the subject matter hereof, and supersedes any prior agreements.

Except to the extent applicable law, if any, provides otherwise, this Agreement shall be governed by the laws of the state of Iowa.

The Parties expressly agree that jurisdiction for any claim or dispute relating to or arising out of this Agreement resides exclusively in the courts of the state of Iowa.

If any provision in this Agreement should be held illegal or unenforceable, such provision shall be modified to the extent necessary to render it enforceable without losing its intent, or severed from this Agreement if no such modification is possible, and other provisions of this Agreement shall remain in full force and effect.

A waiver by either Party of any term or condition of this Agreement or any breach thereof, in any one instance, shall not waive such term or condition or any subsequent breach thereof.

The Parties may not assign or otherwise transfer this Agreement or any rights or obligations herein without the prior written consent of the other Party, which such consent shall not be unreasonably withheld. This Agreement shall be binding upon and shall inure to the benefit of the Parties, their successors and permitted assigns.

Neither Party shall be in default or be liable for any delay, failure in performance (excepting the obligation to pay) or interruption of service resulting directly or indirectly from any cause beyond its reasonable control.

Principal Contacts

Region	**ISAC**
Russell Wood, CICS CEO	**Beth Manley, Compliance Officer**
Phone: 515-663-2928	Phone: (515) 369-7005
E-mail: russell.wood@cicsmhds.org	E-mail: bmanley@iowacounties.org

IN WITNESS THEREOF, this _____ day of _____, 2022, the Parties hereto have set their names and seals by their duly authorized representatives who certify that they are authorized to bind their respective organizations, Central Iowa Community Services Region and ISAC**.**

Central Iowa Community Services Region

_____
By:
Its:

Date: _____

IOWA STATE ASSOCIATION OF COUNTIES

_____
By:
Its:

Date: _____

CICS

Supporting Individuals. Strengthening Communities.

Central Iowa Community Services
POLICIES AND PROCEDURES

FOR

COMPLIANCE WITH THE

HEALTH INSURANCE PORTABILITY

AND ACCOUNTABILITY ACT OF 1996

“HIPAA”

Amended June 2022

TABLE OF CONTENTS

Page

INTRODUCTION

In 1996, Congress enacted the Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA has several provisions; however, the most relevant provisions to the Covered Entity are those directed toward administrative simplification in the health care industry. As part of this effort, Congress enacted significant requirements for health care providers with regard to billing, use and disclosure of Individual information, and security measures to be utilized by entities covered by HIPAA.

Although Congress did establish some requirements in HIPAA itself, it delegated authority to the Secretary of the United States Department of Health and Human Services (the "Secretary") to develop and implement the regulatory scheme. The Secretary has promulgated regulations for the main components of HIPAA's administrative simplification provisions: (1) Transaction Code Set Rules; (2) Privacy Rules; (3) Security Rules; (4) Breach Notification Rules; and (5) Enforcement Rules.

The American Recovery and Reinvestment Act of 2009, included the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). The HITECH Act includes a number of provisions which significantly affect HIPAA covered entities and mandated substantial revisions to the HIPAA regulations. A number of proposed regulations were enacted following HITECH. Then, on January 25, 2013, final HIPAA regulations were published which significantly amended the HIPAA privacy regulations, including changes to the requirement for breach notification, the definition of business associate, business associate obligations, and the definition of protected health information, among other significant changes (the "Final HIPAA regulations"). Together, HIPAA, HITECH, and all related regulations (including the Final HIPAA regulations) shall be referred to in this HIPAA manual as "HIPAA".

The following is a brief summary of each of the main regulatory provisions under HIPAA:

Transactions/Code Sets. One major focus of HIPAA is in the area of electronic data interchange. Specifically, the regulations require all health care providers, health care clearinghouses and health plans who submit electronic transactions to do so in a nationally standardized format. The purpose is to allow for uniformity in claims and other electronic data communications between payors and providers. The regulations apply only to providers who submit transactions electronically. As part of the regulations, the Secretary has published implementation standards for providers to use when transmitting electronic transactions.

Privacy Rule. The HIPAA privacy provisions govern the use and disclosure of an Individual's Individually identifiable health information, known as "protected health information" ("PHI"). These HIPAA privacy regulations are referred to as the "Privacy Rule". To prevent improper use or disclosure of PHI, providers must develop and maintain numerous safeguards, including, but not limited to adopting compliant policies and procedures and training applicable workforce members. The Privacy Rule establishes a foundation of Federal protections for the privacy of PHI. The Privacy Rule does not replace federal, state, or other law that grants Individuals even greater privacy protections, and covered entities are free to retain or adopt more protective policies or practices. In the event state law or the Covered Entity policy is more restrictive than the HIPAA privacy regulations, the more restrictive law or policy will apply.

Security Rule. The HIPAA regulations also address the security of PHI and require covered entities and business associates to adopt administrative, physical and technical safeguards to protect the security of PHI. These HIPAA security regulations are referred to as the "Security Rule". The HIPAA security regulations require organizations to evaluate existing security and confidentiality policies, as well as technical practices and procedures, including access controls, audit trails, physical security and disaster recovery, protection of remote access points, protection of external electronic communications, software discipline and system assessment.

Breach Notification Rule. Under HIPAA, covered entities are required to notify Individuals, the Secretary of HHS, and in some cases, the media, regarding certain breaches of PHI. The term "breach" means the acquisition, access, use or disclosure of PHI in a manner that is not permitted under the privacy regulations, which compromises the security or privacy of the PHI. A breach is presumed to compromise the security or privacy of PHI unless the covered entity can demonstrate through a risk assessment that there is a low probability of compromise to the PHI. In some cases where notice is required, notice of the breach may also be required to be posted on the organization's website, and/or provided to major print or broadcast media. Each covered entity must also maintain a log of breaches, which must be submitted to the Secretary annually, except in cases in which more than 500 Individuals are affected, in which case the Secretary must be notified immediately.

Enforcement Rule. Violations of HIPAA can result in civil monetary penalties and criminal penalties for willful disclosures. While there is no private right of action under HIPAA, Individuals who believe their rights have been violated may file a complaint directly with the HHS Office of Civil Rights. If through preliminary information HHS determines that a violation was likely due to willful neglect, it must conduct an investigation. If founded, HHS is then required to impose a penalty on the violator. State attorneys general can also bring enforcement actions under HIPAA. Civil monetary penalties under HIPAA range from a minimum of $100 per violation to $50,000 per violation for a violation in which the covered entity or business associate did not know and would not have known by exercising reasonable diligence, to a minimum of $1000 per violation to $50,000 per violation for a violation due to reasonable cause, but not willful neglect (with a maximum of $1.5M for violations of identical provisions in a calendar year). For a violation due to willful neglect, the penalty range is a minimum of $10,000, but not more than $50,000 per violation, depending on whether the violation was corrected within 30 days of the date the violator knew or should have known of the violation (up to $.15M for the identical violation in a calendar year), and the penalty could range from a minimum of $50,000 up to $1.5M for an identical violation in a calendar year if the willful neglect violation was not corrected within thirty days. Further, a portion of civil monetary penalty proceeds can be distributed directly to harmed Individuals.

WORKFORCE DESIGNATION

These Policies and procedures cover Central Iowa Community Services. Throughout this document Central Iowa Community Services shall be identified as "Covered Entity"

In accordance with 45 C.F.R. §164.514(d)(2), the Covered Entity has identified:

1) Those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties; and
2) For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

The following designations have been made:

Position/Job Title	PHI Access Required?	Category or Categories of PHI to be accessed	Method of access to PHI
Member County Community Services Directors	Y	Client Information	Hard copies, digital and data systems
Member County Community Services Clerical	Y	Client Information	Hard copies, digital and data systems
Member County Community Services Service Coordinator	Y	Client Information	Hard copies, digital and data systems
Fiscal Agent Auditor	Y	Client Information	Hard copies, digital and data systems
Fiscal Agent Assistant Auditor	Y	Client Information	Hard copies, digital and data systems
Governing Board Member	Y	Client Information	Hard copies, digital and data systems

The Covered Entity shall make reasonable efforts to limit the access of such persons or class of persons identified in this designation to only the minimum necessary access that is required for the person or class of persons to perform their job function.

HYBRID ENTITY DESIGNATION

In accordance with 45 C.F.R. § 164.105(a), the following Covered Entity departments and offices have been designated as healthcare components of the Covered Entity and thus are subject to the HIPAA provisions:

Central Iowa Community Services

The Covered Entity shall ensure that if a member of its workforce performs duties for both a healthcare component and another office or department, that person shall not use or disclose PHI created or received in the course of or incident to the member's work for the healthcare component.

References within this HIPAA Manual to the Covered Entity mean the HIPAA covered entity components of the Covered Entity.

AFFILIATED COVERED ENTITY DESIGNATION

Under 45 C.F.R. §164.105(b), legally separate covered entities may designate themselves as a single affiliated covered entity if all of the covered entities are under common ownership or control. Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity. Common ownership exists if an entity possesses an ownership or equity interest of 5% or more in another entity.

Covered Entity has no common ownership or control.

Accordingly, because they are each part of a single affiliated covered entity under HIPAA, the policies set forth in this manual apply to each entity listed above. Further, any entity formed after the adoption of this policy manual that is under common ownership or control of the Covered Entity will be considered part of the Covered Entity's single affiliated covered entity under HIPAA, whether or not the entity is expressly added to the list of entities set forth above.

However, it is important to note that while the same set of policies and procedures in this HIPAA manual apply to all of the affiliated covered entities designated herein, the affiliated covered entities may only share PHI with each other as permitted under applicable state and federal law.

HIPAA RECORD RETENTION POLICY

I. POLICY

Covered Entity recognizes that HIPAA requires all documentation of HIPAA compliance to be maintained for a period of at least six (6) years. To support Covered Entity's commitment to compliance with HIPAA, Covered Entity shall retain all records documenting HIPAA compliance for at least the required retention period.

II. PURPOSE

The purpose of this policy is to provide Individuals with guidance on the required retention period for HIPAA documents, including examples of the type of records that must be retained.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.530(j)

IV. PROCEDURE

Covered Entity shall retain all documentation of its HIPAA compliance for six years from the date of its creation or the date when it was last in effect, whichever is later. The following are more specific examples of the retention obligations for certain HIPAA compliance records:

A. Accounting of Disclosures

Covered Entity shall retain the following for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later:

1) the information required to be included in an Accounting of Disclosure under HIPAA;

2) all written requests by an Individual for an Accounting of Disclosures; and

3) the written Accounting of Disclosures that is provided to the Individual.

B. Amendment of PHI

Covered Entity shall retain the following for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later:

1) all signed requests to amend PHI for a period of six (6) years;

2) if a request for amendment to PHI is granted, a copy of the material sent to the Individual and/or any third party in response to the amendment; and

3) if a request for amendment is denied, a copy of the written notice of denial, the Individual's statement of disagreement and Covered Entity's rebuttal, if applicable.

C. Business Associate Agreements

Covered Entity shall retain all signed Business Associate Agreements and underlying agreements for a period of at least 6 years from the date of their creation or the date when they last were in effect, whichever is later.

D. De-Identified Information

Covered Entity shall retain all documentation related to HIPAA de-identified data for a period of at least six (6) years from the date of creation or when last in effect, whichever is later.

E. Documentation of HIPAA Uses and Disclosures

Covered Entity shall retain the following for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later:

1) policies and procedures related to the use and disclosure of PHI;

2) all requests for use or disclosure of PHI, including Individual requests for access, amendment and accounting, whether made by the Individual who is the subject of the PHI or third parties;

3) originals or signed copies of agreements with Business Associates referring to the use or disclosure of PHI; and

4) any and all forms related to the use or disclosure of PHI, including but not limited to the following forms:

    a) Authorization to Use or Disclose PHI;
    b) Request to Access PHI;
    c) Request to Amend PHI;
    d) Complaint Form; and
    e) Notice of Privacy Practices and any changes made thereto.

F. Family Involvement/Personal Representatives

Covered Entity shall retain the following for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later:

1) all HIPAA Authorizations to Use or Disclose PHI provided by an Individual's family members; and

2) all documentation provided regarding an Individual's status as a personal representative or guardian of an Individual.

G. Health Oversight Disclosures

Covered Entity shall retain all documentation relating to a use or disclosure which was made to a Health Oversight Agency for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later. This shall include, at a minimum, the following:

1) the name of the person or entity requesting the information;

2) the authority pursuant to which the Individual or entity is requesting the information;

3) the verification procedures used;

4) the circumstances under which the information was sought and released; and

5) the date of the disclosure and a copy of any and all information released.

H. Judicial or Administrative Disclosures

Covered Entity shall retain the following for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later:

1) the original, or a copy, if appropriate, of the court or administrative tribunal's request;

2) statements regarding assurances of notice to the Individual or statements regarding a qualified protective order;

3) the procedures used to verify the identity and authority of the requesting party; and

4) a copy of the PHI provided, if any.

I. Law Enforcement Disclosures

Covered Entity shall retain all documentation relating to a use or disclosure which was made to a Law Enforcement Official for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later. This shall include, at a minimum, the following:

1) the name of the person or entity requesting the information;

2) the authority pursuant to which the Individual or entity is requesting the information, the verification procedures used;

3) the circumstances under which the information was sought and released; and

4) the date of the disclosure and a copy of any and all information released.

J. Limited Data Sets

Covered Entity shall retain all documentation relating to the creation, use or disclosure of a limited data set for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later This shall include, at a minimum, the following:

1) the name of the person or entity receiving the information;

2) the purpose for which the limited data set was created, used or disclosed;

3) the date of the creation, use or disclosure; and

4) a copy of any and all information created, used or disclosed.

K. Marketing

Covered Entity shall retain the following for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later:

1) written marketing policies and any and all revisions to those policies; and

2) all signed Authorizations to use or disclose PHI for marketing; and

3) copies of all marketing materials.

L. Acknowledgement of Receipt of Notice of Privacy Practices

Covered Entity shall retain copies of any written acknowledgments of receipt of the Notice of Privacy Practices, or, if not obtained, documentation of its good faith efforts to obtain such written acknowledgment. Covered Entity must retain this documentation from the date of its creation until six years after the date when it was last in effect.

M. Authorizations

Covered Entity shall retain the signed Authorizations to Use or Disclose PHI for at least six years from the date of its creation or the date when it last was in effect, whichever is later.

N. Notice of Privacy Practices

Covered Entity shall retain a written and electronic copy of each effective HIPAA Notice of Privacy Practices for a period of six years from the date of its creation or if later, the date it was last in effect.

O. Privacy Officer

Covered Entity shall retain the following for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later:

1) the official designation of the Privacy Officer; and

2) the job description for the Privacy Officer.

P. Disclosures Required by Law

Covered Entity shall retain all documentation relating to a use or disclosure which was Required by Law for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later This shall include, at a minimum, the following:

1) the name of the person or entity requesting the information;

2) verification of the identity and/or authority of the Individual requesting the information; and

3) a copy of any and all information released.

Q. Uses and Disclosures of PHI for Research

Covered Entity shall retain all documentation relating to the use and disclosure of PHI for research for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

R. Safeguarding of PHI

Covered Entity shall retain all documentation relating to the safeguarding of PHI for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

S. Sale of PHI

Covered Entity shall retain all documentation relating to the sale of PHI for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

T. Sanctions

Covered Entity shall retain all documentation relating to the investigation of potential violations of HIPAA subject to sanctions and the imposition of sanctions for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

U. Training of Personnel

Covered Entity shall retain all documentation relating to training of personnel for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

V. Verification

Covered Entity shall retain all documentation relating to the verification of the identify and legal authority of a public official or a person acting on behalf of the public official requesting disclosure of PHI for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

W. Breach Notification

Covered Entity shall retain all documentation relating to the risk assessment performed in analyzing a potential breach, a record of all breach notifications provided and a record of all requests for law enforcement delays, for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

HIPAA PRIVACY MANUAL

OVERVIEW: HANDLING USES AND DISCLOSURES OF PHI

I. POLICY

Covered Entity shall Use and Disclose PHI only as permitted under HIPAA. All Covered Entity workforce members should be familiar with HIPAA, the effect of HIPAA on their job functions, and must comply with this Policy at all times.

II. PURPOSE

The purpose of this Policy is to provide Covered Entity workforce with guidance as to the Uses and Disclosures of PHI permitted by HIPAA.

III. REQUIREMENTS AND EXPLANATION

A. Use and Disclosure of PHI is Restricted. Covered Entity workforce may Use or Disclose PHI only as permitted by HIPAA. The permitted Uses and Disclosures are summarized below.

B. Use and Disclosure for Treatment, Payment, or Health Care Operations. Covered Entity may Use PHI for Treatment, Payment or Health Care Operations, without an Authorization, as follows:

1) Covered Entity may Use or Disclose PHI for its own Treatment, Payment or Health Care Operations;

2) Covered Entity may Disclose PHI for Treatment activities of another Health Care Provider;

3) Covered Entity may Disclose PHI to another Covered Entity or Health Care Provider for the Payment activities of the entity that receives the information;

4) Covered Entity may Disclose PHI to another Covered Entity for Health Care Operations of the entity that receives the PHI if (a) Covered Entity and the other Covered Entity had or have a relationship with the subject of the PHI; (b) the PHI pertains to that relationship; and (c) the Disclosure is for one of the following purposes:

   i. Conducting quality assessment and improvement activities (including outcomes evaluation and development of clinical guidelines);
   ii. Population based activities relating to improving health or reducing health care costs;
   iii. Protocol development;
   iv. Case management and care coordination;
   v. Contacting of Health Care Providers and Individuals with information about Treatment alternatives;
   vi. Related functions that do not include Treatment;

vii. Reviewing the competence or qualifications of health care professionals;
viii. Evaluating practitioner and provider performance;
ix. Evaluating health plan performance;
x. Conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to Covered Entity or improve their skills as health care providers;
xi. Training of non-health care professionals;
xii. Accreditation, certification, licensing or credentialing activities;
xiii. Health care fraud and abuse detection or compliance.

5) If Covered Entity participates in an organized health care arrangement, it may Disclose PHI to another participant in the organized health care arrangement for any Health Care Operations of the organized health care arrangement.

C. Use and Disclosure With Authorization. Covered Entity must obtain an Authorization from the Individual who is the subject of PHI before using that PHI for any Use or Disclosure not otherwise provided for under the Privacy Rule. Thus, Covered Entity must obtain an Authorization before using or Disclosing PHI in any manner other than as described in this Policy. The Authorization must be in accordance with the Authorization Policy contained in the Policy Manual.

D. Uses and Disclosures That Require An Opportunity For the Individual To Agree or Object. Covered Entity may Use or Disclose an Individual's PHI for the purposes in this paragraph without authorization, provided that the Individual has been informed in advance of the Use or Disclosure and has an opportunity to agree or prohibit or restrict the Disclosure. Such Uses and Disclosures are for either (a) a facility directory (typically a list of a facility's Individuals); or (b) to discuss an Individual's care with a family member or other person identified by the Individual.

E. Uses and Disclosures That Do Not Require An Opportunity For the Individual To Agree or Object. Covered Entity may Use an Individual's PHI without authorization, and without giving the Individual an opportunity to agree or prohibit or restrict the Disclosure in certain situations specified by the Privacy Rule. These situations are where Use or Disclosure is:

1) <u>REQUIRED BY LAW</u> 45 C.F.R. §164.512(a) (See Required By Law Disclosures Policy)

The Covered Entity may use or disclose PHI to the extent that the use or disclosure is required by law. The Covered Entity will notify an Individual, as required by law, of any such uses or disclosures.

2) <u>PUBLIC HEALTH</u> 45 C.F.R. §164.512(b)

The Covered Entity may disclose PHI for public health activities and purposes that may include:

a) Collecting and receiving information by a public health authority, for the purpose of preventing or controlling disease, injury or disability;
b) Disclosures to a public health authority authorized to receive child abuse or neglect reports;
c) Activities related to the quality, safety or effectiveness of FDA-related products;
d) Contacting Individuals, if authorized by law, who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease; or
e) Disclosing information to an employer, if the Covered Entity provides healthcare to the Individual at the request of the employer to conduct drug testing or to evaluate whether the Individual has a work-related illness or injury.

3) ABUSE OR NEGLECT 45 C.F.R. §164.512(c)

The Covered Entity may disclose PHI to the governmental entity or agency authorized to receive about victims of abuse, neglect or domestic violence, if the Covered Entity believes an Individual has been a victim of abuse, neglect or domestic violence. The disclosure will be made consistent with the requirements of federal and state laws. The Covered Entity will notify the Individual of the disclosure unless, in the exercise of professional judgment, the Covered Entity believes informing the Individual would place them at risk of serious harm.

4) HEALTH OVERSIGHT 45 C.F.R. §164.512(d) (See Health Oversight Uses and Disclosures Policy)

The Covered Entity may disclose PHI to a health oversight agency for activities authorized by law, such as audits, investigations and inspections.

5) LEGAL PROCEEDINGS 45 C.F.R. §164.512(e) (See Judicial or Administrative Purposes Disclosure Policy)

The Covered Entity may disclose PHI in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), in certain conditions in response to a subpoena, discovery request or other lawful process.

6) LAW ENFORCEMENT 45 C.F.R. §164.512(f) (See Law Enforcement Disclosures Policy)

The Covered Entity may disclose PHI for law enforcement purposes, in the following situations:

a) If required by law (ex. reporting wounds or pursuant to a subpoena);
b) Limited information requests for identification and location purposes;
c) Pertaining to victims of a crime;
d) Suspicion that death has occurred as a result of criminal conduct;
e) In the event that a crime occurs on Covered Entity premises; and
f) Medical emergency if it is likely that a crime has occurred.

7) USES AND DISCLOSURES ABOUT DECEDENTS 45 C.F.R. §164.512(g)

a) *Coroners and Medical Examiners*

The Covered Entity may disclose PHI to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law.

b) *Funeral Directors*

The Covered Entity may disclose PHI to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. The Covered Entity may disclose PHI in reasonable anticipation of death.

8) CADAVERIC ORGAN, EYE OR TISSUE DONATION 45 C.F.R. §164.512(h)

The Covered Entity may disclose PHI to organ procurement, banking or transplantation organizations for cadaveric organ, eye or tissue donation purposes.

9) RESEARCH 45 C.F.R. §164.512(i) (See Research Uses and Disclosures Policy)

The Covered Entity may disclose PHI to researchers when their research has been approved by an Institutional Review Board or a Privacy Board that has reviewed the research proposal and established protocols to ensure the privacy of the PHI.

10) AVERTING SERIOUS THREAT TO HEALTH OR SAFETY 45 C.F.R. §164.512(j) (See Serious Threat Disclosures Policy)

Consistent with applicable federal and state laws, the Covered Entity may disclose PHI, if in good faith, it believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. The Covered Entity may also disclose PHI if it is necessary for law enforcement authorities to identify or apprehend an Individual.

11) SPECIALIZED GOVERNMENT FUNCTIONS 45 C.F.R. §164.512(k) (See Specialized Government Functions Uses and Disclosures Policy)

a) *Military and Veterans Activities*

The Covered Entity may disclose PHI of Individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities. The Covered Entity, Veteran's Affairs Department as a component of the Federal Department of Veterans Affairs, may disclose PHI for the purpose of determining eligibility for benefits. The Covered Entity may disclose PHI of an Individual who is foreign military personnel to foreign military authority.

b) *National Security and Intelligence Activities*

The Covered Entity may disclose PHI to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

c) *Correctional Institutions and Other Law Enforcement Custodial Situations*

The Covered Entity may disclose to a correctional institution or law enforcement official PHI for the purposes of providing health care; for the purpose of health and safety of an Individual, other inmates or correctional employees; for the purpose of law enforcement on the premises of the correctional institution or for the administration and maintenance of safety, security and other good order of the correctional institution.

d) *Government Entities Providing Public Benefits*

The Covered Entity as a health plan may disclose PHI relating to eligibility for enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such agencies or the maintenance of such information in a single combined data system accessible to all such agencies is required. In addition, the Covered Entity as a health plan may disclose PHI relating to the program to another covered entity that is a government program providing public benefits if the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate functions of the programs or improve administration and management.

12) WORKERS' COMPENSATION 45 C.F.R. §164.512(l)

PHI may be disclosed by the Covered Entity as authorized to comply with workers' compensation laws and other similar legally established programs.

Special conditions and limitations apply in each of the situations listed above. For example, PHI may be Used or Disclosed for research purposes only upon the approval of an Institutional Review Board or privacy board. The Privacy Officer must be contacted to approve the Use or Disclosure of PHI for any of the above special situations. This Manual will include more comprehensive Policies on some of the above special situations that are more commonly experienced.

F. Disclosures That Require a Business Associate Contract. (See Business Associate Assurances Policy) Whenever Covered Entity engages a third party to perform or assist in the performance of Covered Entity's activities which may involve the use or disclosure of PHI to such third party, Covered Entity will need to enter into a "Business Associates Agreement" with such party. Covered Entity may Disclose PHI to a Business Associate, or allow the Business Associate to create or receive PHI on Covered Entity's behalf, if the Business Associate enters into a contact with Covered Entity assuring that the Business Associate will appropriately safeguard the PHI. See Covered Entity's Business Associate Assurances Policy for more information on this issue.

G. Disclosures of Limited Data Sets. (See Limited Data Set Policy) Covered Entity may Use or Disclose PHI that meets the definition of a Limited Data Set only if Covered Entity enters into a Data Use Agreement with the recipient of the Limited Data Set, and if the recipient will use the Limited Data Set only for research, public health or Health Care Operations. Covered Entity may Use PHI to create a Limited Data Set, and may Disclose PHI to a Business Associate to create a Limited Data Set.

If Covered Entity personnel become aware of a pattern of activity that constitutes a material breach or violation of a Data Use Agreement, the personnel should notify the Privacy Officer, who will

take reasonable steps to cure the breach or end the violation. If these steps are unsuccessful, Disclosure of PHI to the Limited Data Set recipient must be discontinued and the violation must be reported to the Secretary of the Department of Health and Human Services.

Covered Entity may Disclose De-identified data without an Authorization only after it has been properly De-identified in accordance with the De-Identification Policy in this Manual.

Limited Data Sets will be released only to organizations that have signed a Data Use Agreement that satisfies the Privacy Rule requirements and the identifying data has been removed as required by the Privacy Rule. Limited Data Sets will be used only for research, public health, or Health Care Operations purposes.

1) Definition of Limited Data Set: A Limited Data Set is PHI that excludes the following direct identifiers of subject of the PHI, or of relatives, employers, or household members of the subject of the PHI: (i) names; (ii) postal address other than town, city, state and zip code; (iii) telephone numbers; (iv) fax numbers; (v) e mail address; (vi) social security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) web universal resource locators; (xiv) internet protocol address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images.

2) Data Use Agreement. Covered Entity may Use or Disclose a Limited Data Set ("LDS") only if Covered Entity enters into an agreement with the recipient of the Limited Data Set that:

   a) Establishes the permitted Uses and Disclosures of the LDS by the recipient;
   b) Does not allow the recipient to Use or Disclose the LDS in a manner that would violate the Privacy Rule if done by Covered Entity;
   c) Establishes who is permitted to Use or Receive the LDS; and
   d) Provides that the LDS recipient will:

      i. Not Use or Disclose the LDS other than as permitted by the agreement or otherwise required by law;
      ii. Use appropriate safeguards to prevent Use or Disclosure of the information other than as provided for by the agreement;
      iii. Report to Covered Entity any Use or Disclosure of the LDS not provided for by the agreement;
      iv. Ensure that any agents, including a subcontractor, to whom it provides the LDS agrees to the same restrictions; and
      v. Not identify the information or contact the Individuals.

If Covered Entity becomes aware of a pattern of activity of the LDS recipient that constitutes a material breach or violation of the data use agreement, Covered Entity must take reasonable steps to cure the breach or end the violation. If these steps are unsuccessful, Covered Entity must discontinue Disclosure of PHI to the LDS recipient and report the problem to the Secretary of Health and Human Services (or her designee).

H. The Minimum Necessary Standard. (See Minimum Necessary Policy) The minimum necessary standard applies to all of Covered Entity's Uses and Disclosures of PHI except to (1) Disclosures to or requests by a health care provider when the PHI will be Used for Treatment purposes; (2) Disclosures to the Individual who is the subject of the PHI; or (3) Uses or Disclosures made pursuant to an Authorization requested by the Individual.

Covered Entity shall limit Use or Disclosure of PHI to the "minimum necessary," as set forth in guidance that the Secretary of the Department of Health and Human Services will issue. Until the issuance of such guidance, Covered Entity shall limit Use and Disclosure of PHI, to the extent practicable, to the Limited Data Set, or, if needed, to the minimum necessary to accomplish the intended purpose.

When Using or Disclosing PHI, or when requesting PHI from another entity, Covered Entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure or request for health information. Covered Entity must implement the following requirements after assessing their own unique circumstances. The requirements do not require limiting PHI Use or Disclosure to only what is absolutely the minimum necessary amount, but rather to what may reasonably be necessary to accomplish the purpose of the Use or Disclosure.

1) Covered Entity personnel's access to PHI. Covered Entity must identify those persons or classes of persons in its workforce who need access to PHI to carry out their duties. For each such person or class of persons, Covered Entity must identify the category or categories of PHI to which access is needed, and any appropriate conditions to such access. Covered Entity must make reasonable efforts to limit the access to PHI of such identified persons or classes of persons to the identified categories of PHI.

2) Minimum Necessary Disclosure of PHI.

   a) For Disclosures made on a routine and recurring basis, Covered Entity must implement a standard protocol that limits the Disclosure to PHI reasonably necessary to achieve the purpose of the Disclosure.
   b) For non-routine Disclosures, Covered Entity must develop criteria for determining and limiting such Disclosure to the minimum necessary PHI to accomplish the purpose of the non-routine Disclosure. Such Disclosures must be reviewed on a case by case basis in accordance with these criteria.

3) Minimum Necessary Requests for PHI.

   a) For requests for PHI made on a routine and recurring basis, Covered Entity must implement a standard protocol that limits the Disclosure to PHI reasonably necessary to achieve the purpose of the Disclosure.
   b) For non-routine requests, Covered Entity must develop criteria for determining and limiting Disclosure to the minimum necessary PHI to accomplish the purpose of the non-routine Disclosure. Such requests must be reviewed on a case by case basis in accordance with these criteria.

4) Reasonable Reliance. Covered Entity may rely on a requested Disclosure for PHI as being the minimum necessary for a stated purpose when the request is made by:

a) A public health official or agency for a Disclosure permitted under the Privacy Rule;
b) Another Covered Entity;
c) A professional who is a workforce member or Business Associate of the Covered Entity holding the PHI; or
d) A researcher with appropriate documentation from an Institutional Review Board or Privacy Board.

I. Other Permitted Uses and Disclosures. Covered Entity may also Use or Disclose PHI as follows:

1) Covered Entity may Disclose PHI to the subject of the PHI;

2) Covered Entity may Use or Disclosure PHI incident to a Use or Disclosure permitted or required by the Privacy Rule, provided that Covered Entity has complied with the Minimum Necessary requirements and enacted reasonable safeguards to prevent the intentional or unintentional Use or Disclosure of PHI that is not in compliance with the Privacy Rule.

J. Mental Health Information and Other Situations in Which Iowa Law Provides Greater Protection for Data. (See the Iowa Laws Providing Greater Protection Policy for further information.) One example of an Iowa law that provides greater protection for information than does HIPAA, is Iowa's Mental Health Privacy Law at Iowa Code §228. Therefore, before disclosing Mental Health Information, the Covered Entity must confirm with the Privacy Officer that such disclosure is permitted under Iowa's Mental Health Privacy Law at Iowa Code §228. Mental Health Information is defined as oral, written, or recorded information which indicates the identity of an Individual receiving professional services and which relates to the diagnosis, course, or treatment of the Individual's mental or emotional condition. Covered Entity shall not disclose Mental Health Information except as set out in this policy and in compliance with Iowa law regarding the disclosure of Mental Health Information.

IOWA LAWS REQUIRING GREATER PROTECTIONS POLICY

I. POLICY

HIPAA is meant to be comprehensive and uniform throughout the United States. However, HIPAA does not repeal (or "preempt") any state laws that are not contrary to the provisions of HIPAA, which: (1) are related to the privacy of individually identifiable health information that are more stringent than HIPAA; (2) provide for the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention; (3) require a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals; or (4) are approved based upon a determination of the Secretary.

II. PURPOSE

The purpose of this policy is to provide greater clarification regarding *some* of the most common Iowa laws that are more protective than HIPAA, and thus, which must also be followed when using or disclosing certain information. For additional information on the Iowa legal HIPAA preemption analysis, refer to the following document which further analyzes HIPAA preemption under many Iowa laws:

http://www.iowamedical.org/documents/legal/IowaHIPAAPreemptionAnalysis.pdf

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §160.203
- Iowa Code §228
- Iowa Code §125
- 42 U.S.C. 290dd-2
- 42 C.F.R. Part 2
- Iowa Code §141A

IV. REQUIREMENTS AND EXPLANATION

A. Mental Health Information Iowa Code §228.

1) Definitions:

   a) Mental Health Information is defined as oral, written, or recorded information which indicates the identity of an Individual receiving professional services and which relates to the diagnosis, course, or treatment of the Individual's mental or emotional condition.

   b) Professional Services means diagnostic or treatment services for a mental or emotional condition provided by the mental health professional.

2) Covered Entity shall not disclose Mental Health Information except as set out in this policy and in compliance with Iowa law regarding the disclosure of Mental Health Information.

3) In addition to the HIPAA rules governing the disclosure of PHI, the following rules apply to disclosures of Mental Health Information:

a) Voluntary Authorization. An Individual eighteen years of age or older, or an Individual's legal representative, may consent to the disclosure of Mental Health Information relating to the Individual by signing a voluntary authorization form.

i. The authorization form shall:

1) Specify the nature of the Mental Health Information to be disclosed;
2) State the persons or type of persons authorized to disclose the information;
3) State the purposes for which the information may be used both at the time of the disclosure and in the future;
4) Advise the Individual of the Individual's right to inspect the disclosed mental health information at any time;
5) State that the authorization is subject to revocation and state the conditions of revocation;
6) Specify the length of time for which the authorization is valid; and
7) Contain the date on which the authorization was signed.

ii. A copy of the authorization shall be provided to the Individual or to the legal representative of the Individual authorizing the disclosure, and must be included in the Individual's record of Mental Health Information.

iii. An Individual or an Individual's legal representative may revoke a prior authorization by providing a written revocation to the recipient named in the authorization and to the Individual/entity previously authorized to disclose the Mental Health Information. The revocation is effective upon receipt of the written revocation by the person previously authorized to disclose the Mental Health Information. After the effective revocation date, Mental Health Information shall not be disclosed pursuant to the revoked authorization. However, Mental Health Information previously disclosed pursuant to the revoked authorization may be used for the purposes stated in the original written authorization.

b) Disclosures in the Event of Medical Emergency or for Medical or Mental Health Professional Services.

i. A recipient of Mental Health Information shall not disclose the information received, except as specifically authorized for initial disclosure. However, Mental Health Information may be transferred at any time to another facility, physician, or mental health professional in cases of a medical emergency or if the Individual or

the Individual's legal representative requests the transfer in writing for the purposes of receipt of medical or mental health professional services, at which time the requirements of this policy regarding the disclosure of mental health information shall be followed.

c) Disclosures to Providers of Professional Services and Administrative Disclosures.

i. An Individual shall be informed that informed that Mental Health Information relating to the Individual may be disclosed to employees or agents of the or for the same mental health facility, or to other providers of professional services or their employees or agents if and to the extent necessary to facilitate the provision of administrative and professional services to the Individual.

ii. Mental health professionals or facilities may disclose administrative information necessary for the collection of fees, to a person or agency providing collection services, as well as additional information in civil litigation related to the collection when necessary to respond to a motion by the Individual for greater specificity or to dispute a defense or counterclaim.

iii. Mental health professionals or facilities may disclose Mental Health Information if necessary for the purpose of conducting scientific and data research, management audits, or program evaluations of the mental health professional or facility, only to persons who have demonstrated and provided written assurance of their ability to ensure compliance with Iowa Code §228.

iv. Mental Health Information may be disclosed to other providers of professional services or their employees or agents if and to the extent necessary to facilitate the provision of administrative and professional services to the Individual.

d) Compulsory Disclosures.

i. Iowa Code §228.6 includes a number of situations in which mental health professionals or facilities may disclose Mental Health Information in order to meet certain requirements under Iowa laws, or to meet the compulsory reporting or disclosure requirements of other state or federal law relating to the protection of human health and safety.

e) Disclosures for Claims Administration and Peer Review.

i. Mental Health Information may be disclosed by a mental health professional, data collector, mental health facility to a third party payor or to a peer review organization if:

1) The Individual or legal representative has given prior written consent; and

2) The third party payor or the peer review organization has filed a written statement with the Iowa Commissioner of Insurance in which the filer agrees to certain conditions. Note that self-insured employers that have not filed such statement shall not be granted routine or ongoing access to Mental Health Information unless the employees or agents have signed a statement indicating that they are aware that the information shall not be used or disclosed except as provided under Iowa law and that they are aware of the penalty for unauthorized disclosure.

ii. Third party payors and peer review organizations shall not use or disclose Mental Health Information to any person, except as necessary to administer claims submitted or to be submitted for payment to the third party payor, to conduct a utilization and quality control review of mental health care services, to conduct an audit of claims paid, or as otherwise authorized by law.

f) Disclosures to Family Members.

i. A mental health professional or facility may disclose Mental Health Information to the spouse, parent, adult child, or adult sibling of an Individual who has a chronic mental illness if all of the following conditions are met:

1) The disclosure is necessary to assist in the provision of care or monitoring of the Individual's treatment;
2) The spouse, parent, adult child, or adult sibling is directly involved in providing care to or monitoring the treatment of the Individual; and
3) The involvement of the spouse, parent, adult child, or adult sibling is verified by the Individual's attending physician, attending mental health professional, or a person other that the spouse, parent, adult child, or adult sibling who is responsible for providing treatment to the individual.

ii. A request for Mental Health Information by a person authorized to receive such information under this section shall be in writing, except in an emergency as determined by the mental health professional verifying the involvement of the spouse, parent, adult child, or adult sibling.
iii. Unless the Individual has been adjudged incompetent, the person verifying the involvement of the spouse, parent, adult child, or adult sibling shall notify the Individual of the disclosure.
iv. The Mental Health Information that can be disclosed under this section is limited to the following:

1) A summary of the Individual's diagnosis and prognosis;

2) A listing of the medication which the Individual has received and is receiving and the Individual's record of compliance in taking medication prescribed in the previous six months; and
3) A description of the Individual's treatment plan.

g) Disclosures of Psychological Test Material.

i. Unless otherwise permitted under Iowa Code §228, a person in possession of psychological test material shall not disclose the test material to any other person, including in any administrative, judicial or legislative proceeding. However, in accordance with HIPAA, the Individual who is the subject of the test material has a right to access the material. Also, if the Individual so requests in writing and completes a written authorization, all records associated with a psychological test of the Individual shall be disclosed to a psychologist licensed under Iowa Code §154B who is designated by the Individual.

h) Record of Disclosures. Upon the disclosure of Mental Health Information, the person disclosing the mental health information shall enter a notation on and maintain the notation with the Individual's record of Mental Health Information, stating the date of the disclosure and the name of the recipient of Mental Health Information.

i) Statements to Recipients. Further, the person disclosing Mental Health Information shall give the recipient of the information a statement which informs the recipient that disclosures may only be made pursuant to the written authorization of an Individual or an Individual's legal representative, or as otherwise provided under state and federal law, that the unauthorized disclosure of mental health information is unlawful, and that civil damages and criminal penalties may be applicable to the unauthorized disclosure of Mental Health Information.

B. Chemical or Substance Abuse Iowa Code § 125

1) A physician or any person acting under the direction or supervision of a physician, or a Facility (as defined under Iowa Code §125.2) shall not report or disclose to any law enforcement officer or agency, the name of an Individual who has applied for voluntary treatment or rehabilitation services for substance abuse, or the fact that the treatment was requested or undertaken, nor shall such information be admissible as evidence in any court, grand jury or administrative proceeding unless authorized by the Individual seeking treatment.

2) Further, if a minor personally makes application seeking such treatment, the fact that the minor sought treatment or rehabilitation or is receiving treatment or rehabilitation services shall not be reported or disclosed to the parents or legal guardian of such minor without the minor's consent.

3) The registration records and other records of Facilities are confidential and privileged to the Individual patient. However, the director of the Iowa Department of Public Health may make available information from patient's records for purposes of research into the causes and treatment of substance abuse as long as the information does not disclose any Individual's name or other identifying information.

4) However, a patient's records may be disclosed to medical personnel in a medical emergency with or without patient consent.

5) Records of the identity, diagnosis, prognosis, or treatment of a person which are maintained in connection with the provision of substance abuse treatment services are confidential under Iowa law. Further, under federal law, 42 U.S.C. 290dd-2 and 42 C.F.R. Part 2, there are additional restrictions on disclosures of drug abuse information obtained by a federally assisted drug abuse program, that must be followed by third party payors with regard to records disclosed to them by federally assisted alcohol or drug abuse programs, entities having direct administrative control over such programs, and persons who receive patient records directly from such programs who are notified of the restrictions on redisclosure of the records. These federal laws should be reviewed carefully to determine if and how they apply in each circumstances involving patient records regarding drug or alcohol abuse treatment.

6) *Notice to accompany disclosure.* Each disclosure made with the patient's written consent must be accompanied by the following written statement: "This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient."

C. HIV/Acquired Immune Deficiency Syndrome Iowa Code § 141A.

1) Any information related to HIV or AIDS tests, including reports and records obtained, submitted or maintained pursuant to Iowa Code §141A is strictly confidential medical information and shall not be disclosed except as provided under Iowa Code §141A.

2) Iowa Code §141A includes numerous provisions addressing when, and under what circumstances, HIV/AIDS information can be disclosed. Confidential information disclosed pursuant to Iowa Code §141A should include a notice to the recipient that the recipient must continue to maintain the confidentiality of the information and that the recipient must not further disclose the information without a specific authorization of the Individual or as otherwise permitted by law. A general authorization for the release of HIV/AIDS information is not sufficient, thus any authorization form must include an opportunity for the Individual to specifically authorize the release of such information.

ACCESSING PHI POLICY

I. POLICY

Covered Entity recognizes that Individual rights are a critical component to maintaining quality care and service, and is committed to allowing Individuals to exercise their rights under applicable federal, state and/or local laws and regulations. To support this commitment, Covered Entity maintains written Policies and Procedures to provide guidance when faced with a request by an Individual for access to his or her PHI.

II. PURPOSE

The purpose of this policy is to provide Individuals with access to PHI when such access is required and appropriate.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.524

IV. PROCEDURE

A. General Rule

Under the Privacy Rule, Individuals may request access to their PHI which is found in the records Covered Entity keeps. Covered Entity, in most situations, is obligated to provide the Individual with the requested information. This access may be in various forms, including allowing the Individual to inspect and/or obtain a copy of the PHI held by Covered Entity, including electronic copies if possible. In certain situations, Individuals are not entitled to have access to the requested information, which are set forth in greater detail below. If the request for access is denied, an Individual may be entitled to a review of that denial. It is anticipated that most requests for access to an Individual's PHI will be accommodated. However, in some situations, the determination will be made to deny access. This Policy is designed to set forth the procedures Covered Entity should follow in responding to a request for access.

B. Processing Requests

Because of the many complexities surrounding a request for access under the Privacy Rule, it is Covered Entity's Policy to refer requests for access to Russell Wood or designee who will review the request to determine if the Individual is eligible to receive requested PHI. His contact information is:

Russell Wood
russell.wood@cicsmhds.org
123 1st Ave SW, (PO Box58)
Hampton IA 50441
641-456-2128
Fax 641-456-2852

C. Form of Request

Covered Entity shall request that the Individual requesting access to PHI complete an appropriate form.

D. Response Time for Request for Access

1) *Respond Within Thirty Days*. Upon receipt of the request to access PHI, Covered Entity will, within thirty (30) days: (a) inform the Individual of the acceptance of the request to provide access and provide the access requested; or (b) provide the Individual with a written denial.

2) *One Thirty Day Extension*. In certain circumstances, Covered Entity may extend the time required to respond to the request by an additional thirty (30) days as long as: (1) Covered Entity, within thirty days, provides the Individual with a written statement of the reasons for the delay and the date by which the Covered Entity will complete its action on the request; and (2) Covered Entity may only have one such delay per request. This delay should be the exception and not the rule, however, and the reason for delay in responding to the request for access must be documented and retained by the Covered Entity.

E. Approving Request for Access

1) *All Access*. Covered Entity will provide the Individual with access to the PHI in the form or format requested by the Individual, if the PHI is readily reproducible in such form or format. If the information is not readily reproducible in the form or format requested, then Covered Entity will provide the Individual with access to the PHI in a readable hard copy form or such other form as agreed to by the Individual and Covered Entity.

2) *Electronic Access*. If Covered Entity maintains one or more Designated Record Sets in electronic form, then an Individual has the right to receive a copy of the PHI maintained electronically in the Designated Record Sets in the electronic form and format the Individual requests, if readily producible in that form and format. If not readily producible in the electronic form and format requested, the Individual has the right to receive such PHI in another readable electronic format as the Individual and Covered Entity agree.

3) *Inspection/Mailing*. If requested by the Individual, Covered Entity will arrange with the Individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing of the PHI within the specified time period.

4) *Summary*. A summary of the requested PHI may be provided in lieu of access to the information only when the Individual had agreed to such summary in advance, and to any related fees imposed.

5) *Designated Person*. If the Individual directs the Covered Entity to transmit a copy of the PHI directly to another person, Covered Entity must provide a copy to such

person. However, Covered Entity should ensure that the Individual designated the other person in writing and clearly specified where to send the PHI.

6) *Written Approval*. If Covered Entity approves the request for access, the Access Request Form must be completed by Covered Entity including signature and date noting acceptance of the request to access.

F. Denying Request for Access

Covered Entity may deny the Individual's request for access in certain situations, some of which will trigger the right to have the denial reviewed, in accordance with the criteria described below.

1) *Unreviewable Grounds for Denial of Access to PHI.*

The Covered Entity may deny an Individual access to PHI, without providing the Individual an opportunity for review, for the following reasons:

a) Individuals have a right of access to inspect and obtain PHI (PHI) about the Individual in a designated record set, for as long as the information is maintained by the Covered Entity, except for:

i. Psychotherapy notes;
ii. Information compiled in reasonable anticipation of, or for use in, a legal proceeding; or
iii. PHI maintained by the Covered Entity that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988 (CLIA).

b) The Covered Entity is a health care provider acting under the direction of a correctional institution and has determined that the requested information would jeopardize the health, safety, security, custody or rehabilitation of the Individual or other inmates, or the safety of a correctional employee or other person responsible for transporting the Individual;

c) The information requested was obtained under a promise of confidentiality from someone other than the Covered Entity and the inspection or copying will likely reveal the source of the information;

d) The PHI is obtained by the Covered Entity in the course of research that includes treatment of the research participants, while such research is in progress. For this exception to apply, the Individual must have agreed to the denial of access in conjunction with the Individual's consent to participate in the research and the covered provider must have informed the Individual that the right of access will be reinstated upon completion of the research; or

e) The PHI requested is also subject to the Privacy Act set out in federal law at 5 U.S.C. §552a.

2) *Reviewable Grounds for Denial of Access to PHI*

The Covered Entity shall provide the Individual with a right to review the following reasons for denial:

a) If a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the Individual or another person;

b) the PHI requested makes reference to someone other than the Individual (unless such person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause serious harm to that other person; or

c) The request is made by an Individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the Individual or another person.

3) **Response to the Individual in the Event of a Decision to Deny Access**

a) *Written Notice of Denial.* If Covered Entity has determined that it will deny the Individual's request for access, Covered Entity will provide a timely (per the time frames required under this Policy), written denial to the Individual. The denial shall be written in plain language and shall include: (i) the basis for the denial; (ii) if applicable, the statement of the Individual's right to have the denial reviewed, including a description of how the Individual can exercise these rights; and (iii) a description of how the Individual may complain to Secretary of Health and Human Services, including the name or title and telephone number of the contact person.

b) *Procedure in Grounds for Review*. If access is denied and the Individual has grounds for review, the Individual has the right to have a denial reviewed by a licensed health care professional who is designated by the Covered Entity to act as a reviewing official and who did not participate in the original decision to deny access. If the Individual requests such review, the Covered Entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested. The Covered Entity must provide or deny access in accordance with the determination of that official, and must promptly notify the Individual of the determination.

G. Fees

Covered Entity may assess a fee to the Individual for the costs associated with granting access to the requested PHI. Fees shall be reasonable and based on cost and may only be assessed for the costs associated with:

1) Labor for copying the PHI requested by the Individual whether in paper or electronic form;

2) Supplies for creating the paper copy or electronic media if the Individual requests that electronic copy be provided on portable media;

3) Postage when the Individual had requested the copy or the summary or explanation be mailed; and

4) Preparing an explanation or summary of the PHI. The fee may not include costs associate with searching for and retrieving the requested information.

H. Documentation and Record Retention Requirements:

1) *Forms*. Covered Entity shall retain a copy of the signed Request to Access PHI form for a period of six (6) years.

2) *Responses to Requests*. If a request for access to PHI is granted, the Covered Entity will maintain a copy of the material sent to the Individual and/or any third party in response to the request for access. If a request for access is denied, the Covered Entity will maintain a copy of the written notice of denial, the Individual's statement of disagreement and the Covered Entity's rebuttal, if applicable. All documentation required under this section must be retained for a period of at least six (6) years.

INSTRUCTIONS FOR RESPONDING TO REQUESTS FOR ACCESS

1) Provide the Individual with a Request to Access PHI Form.
2) Inform the Individual that the Covered Entity will notify the Individual of its decision.
3) Inform the Individual of the grounds on which the Covered Entity can deny access.
4) Send the Individual written notice of acceptance or denial.
5) If request is accepted, allow Individual to obtain requested information.
6) Upon releasing information, any documents released will have the client name highlighted on each page of information released in order to identify that each page of the information being released belongs to that record set.
7) Place all denials or acceptances in the Individual's designated record set.

SEE INDIVIDUAL REQUEST FOR PHI FORM AND NOTICE OF DECISION REGARDING REQUEST FORM ATTACHED TO THIS HIPAA MANUAL

INDIVIDUAL REQUEST FOR PHI

This form constitutes an Individual's request for PHI (PHI) held by the Covered Entity. To obtain your PHI this form must be filled out in its entirety.

Name: (First/Middle/Last) _____
Address: (Street/City/State/Zip code) _____
Date of Birth: (Month/Day/Year) _____
Social Security Number: _____ Date of Request: _____

I REQUEST THE COVERED ENTITY TO PROVIDE ME ACCESS TO THE FOLLOWING PHI ABOUT ME:

☐ Mental Health Records
☐ Medical Records
☐ Billing Records
☐ Other _____

I REQUEST ACCESS TO MY PHI FOR THE DATES COVERING THE FOLLOWING TIME PERIOD(S):

From: (Month/Day/Year) _____ to: (Month/Day/Year) _____

I WOULD LIKE TO OBTAIN THE REQUESTED PHI IN THE FOLLOWING FORMAT:

☐ Electronic sent to the following address: _____
☐ Hardcopy sent to the following address: _____
_____
☐ Other: _____
☐ On-site inspection

I UNDERSTAND THE COVERED ENTITY MAY CHARGE A REASONABLE FEE FOR THE COSTS OF COPYING, MAILING OR OTHER SUPPLIES ASSOCIATED WITH MY REQUEST.

_____
Signature of Individual Date

IN THE EVENT THIS REQUEST IS MADE BY THE INDIVIDUAL'S PERSONAL REPRESENTATIVE

_____
Signature of Personal Representative Date

_____
Legal Authority of the Personal Representative

NOTICE OF DECISION REGARDING INDIVIDUAL REQUEST FOR PHI

YOUR REQUEST TO ACCESS THE FOLLOWING PHI (PHI),

☐ Mental Health Records
☐ Medical Records
☐ Billing Records
☐ Other _____

FOR PHI COVERING THE DATES OF: ____/____/_____ through ____/____/_____

IN THE FOLLOWING FORMAT:

☐ Copies of requested information (Cost $____.__)
☐ Inspection of my health information at THE COVERED ENTITY.

HAS BEEN:

☐ **Accepted**

[List procedure for receiving copies or a date to inspect the PHI at the facility here]

☐ Denied

Reason for Denial:

☐ You do not have a right to access the information nor to request a review of this decision as it falls under the following category:

- Psychotherapy notes;
- PHI requested is related to civil, criminal, or administrative action;
- PHI requested is subject to or exempt from the Clinical Laboratory Improvements Amendments of 1988 (CLIA);
- You are an inmate and the PHI requested could jeopardize the health, safety, security, custody or rehabilitation of yourself or others;
- You have agreed to participate in research and have been notified that this information is restricted while in the course of the research. You may access the information upon completion of the research;
- the PHI requested is subject to the Privacy Act;
- The PHI requested was obtained from a third party (non-health care provider) under condition of confidentiality.

☐ Your request has been denied for the following reason: (Note: you may request a review of this decision by following the appeal procedure outlined on this decision.)

- A licensed Health Care Professional has determined that the access requested is likely to endanger the life or physical safety of yourself or others;
- the PHI requested makes reference to someone else and is likely to cause that person serious harm;
- As a personal representative it is believed that access to the requested PHI may subject the Individual you represent to domestic violence, abuse or neglect or may endanger their life or is not in the best interest of the Individual represented.

☐ Other: _____

Staff Signature: _____ Date:_____

Date Request Received: _____

REQUEST FOR REVIEWS

You may have this decision reviewed by sending a written request to:

Russell Wood
russell.wood@cicsmhds.org
123 1st Ave SW, (PO Box58)
Hampton IA 50441
641-456-2128
Fax 641-456-2852

The request must be received within 10 days from the above date. The review process is described below:

REVIEW PROCEDURE

The purpose of this section is to describe how the Covered Entity's decisions can be reviewed.

- If you disagree with this notice of decision you may seek a review of the decision. Only reviews initiated by you or your personal representative will be evaluated.

- To request a review, you must send a written notice requesting a review within ten (10) working days of receipt of your Notice of Decision.

- Within ten (10) working days of the receipt of the written request for a review, the Covered Entity shall send you a written notice informing you of the date, time and place that will review will be conducted.

- A written decision will be issued no later than ten (10) working days after the review proceeding. A copy of that decision will be sent to you and your representative (if applicable). A notice explaining the effect of the decision regarding access to your private health information and your rights regarding any subsequent review will accompany the decision.

- The review proceeding shall be held privately. At any review, you have the right to be present and have an attorney or other advocate accompany and represent you at your own expense. If you cannot afford an attorney, you may contact Legal Services Corporation of Iowa, the Iowa Volunteer Lawyer Project, or Disability Rights IOWA, for assistance.

DOCUMENTING USES AND DISCLOSURES OF PHI POLICY

V. POLICY

Covered Entity is committed to ensuring the privacy and security of Individuals' PHI and appropriately documenting the various Policies, Procedures and other administrative requirements of HIPAA.

VI. PURPOSE

The purpose of this policy is to provide guidance and ensure compliance with provisions of HIPAA related to maintenance of Policies, Procedures and other administrative requirements.

VII. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.530(i)
- 45 C.F.R. §164.530(j)

VIII. PROCEDURE

A. Administrative Requirements under the Privacy Rule. The Privacy Rule requires Covered Entity to develop and implement Policies and Procedures related to PHI that are designed to comply with the standards under the Privacy Rule, as from time to time amended. Covered Entity must maintain documentation, in written or electronic form, of Policies, Procedures communications and other administrative documents as required by the Privacy Rule for a period of at least six years from the date of creation or the date when last in effect, whichever is later.

B. Changes in the Privacy Rule or Other Laws. Covered Entity will promptly incorporate into its policies, procedures and other administrative documents any and all changes in the Privacy Rule and other federal, state and/or local laws that relate to the use and/or disclosure of PHI.

C. Changes to Policies, Procedures or Other Administrative Documents. If a policy, procedure or other administrative document is changed as a result in a change in practice or a change in law, the changes shall be documented and implemented as soon as is reasonably practicable.

D. Specifics of Requirements Related to Documentation. Covered Entity will maintain the following documentation in an organized manner:

1) Requests for use or disclosure of PHI, including Individual requests for access, amendment and accounting, whether made by the Individual who is the subject of the PHI or third parties;

2) Originals or signed copies of agreements with Business Associates referring to the use or disclosure of PHI;

3) All of Covered Entity's Policies, Procedures, and protocols required by the Privacy Rule, including policies related to the use and disclosure of PHI; and

4) Any and all forms related to the use or disclosure of PHI, including but not limited to the following forms:

   a) Authorization to use or disclose PHI;
   b) Request to Access PHI;
   c) Request to Amend PHI;
   d) Complaint Form; and
   e) Notice of Privacy Practices and any changes made thereto.

E. Security of Documentation. Documentation shall be maintained in a secure manner, with access appropriately limited to those Covered Entity employees authorized to access the documentation.

ACCOUNTING OF DISCLOSURES POLICY

I. POLICY

Covered Entity recognizes that Individual rights are a critical component to maintaining quality care and service, and is committed to allowing Individuals to exercise their rights under applicable federal, state and/or local laws and regulations. To support this commitment, Covered Entity maintains written Policies and Procedures to provide guidance to Covered Entity workforce members when faced with a request by an Individual for an accounting of the uses and disclosures of PHI Covered Entity has made.

II. PURPOSE

The purpose of this policy is to provide guidance in responding to an Individual's request for an accounting in accordance with the Privacy Rule and HITECH.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R §164.528
- Section 13405(c) of HITECH

IV. PROCEDURE

A. Right to an Accounting

An Individual has the right to receive an accounting of disclosures of PHI made by the Covered Entity in the 6 years prior to the date on which the accounting was requested, except for disclosures:

1) To carry out treatment, payment and health care operations (except, if and when required by HITECH[1]);

[1] HITECH provides that the exception in the HIPAA accounting rule for disclosures for treatment, payment and health care operations no longer applies to disclosures made through an electronic health record (the "TPO Disclosures"). While HITECH significantly expands an Individual's right to information by including TPO Disclosures in the accounting rule (which likely encompass most disclosures made about Individuals), HITECH also states that an Individual only has a right to receive an accounting of such TPO Disclosures made during the three-year period prior to the date of the request (rather than the six-year time period currently provided under the accounting rules). On May 31, 2011, the Department of Health and Human Services ("HHS") published a Notice of Proposed Rulemaking ("NRPM"), proposing amendments to the HIPAA rules on accounting of disclosures in order to implement the statutory requirements under HITECH (described above). 76 Fed. Reg. 31426 (May 31, 2011). The NPRM proposes to amend HIPPA in two respects: (1) It makes several changes to the current rules on accounting of disclosures of protected health information; (2) It adds an Individual right to receive an access report indicating who has accessed (including both uses and disclosures) protected health information maintained in an electronic designated record set, about the Individual. The proposed accounting rules and access report rules have been the subject of great controversy due to the substantial administrative burdens the proposals were perceived to create for covered entities and business associates. Notably, HHS did not include these proposals in the final HIPAA rules that were published this year on January 25, 2013. HHS has advised that the HITECH Act's mandate to amend the HIPAA rules on accounting of disclosures will be the subject of future rulemaking, with no specific future date announced. It is unknown whether HHS will proceed with the same (controversial) rules it proposed in

2) To Individuals of PHI about them;

3) Incident to a use or disclosure otherwise permitted[2];

4) Pursuant to an authorization;

5) For national security;

6) To correctional institutions or law enforcement officials;

7) As part of a limited data set; or

8) If it occurred prior to the compliance date for the Covered Entity.

The Covered Entity shall temporarily suspend an Individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, at the request of a health oversight agency or law enforcement official, if the Covered Entity is provided a written statement that such accounting would be reasonably likely to impede the agency's action. In addition, the agency must also state a time for which the suspension is required. If the statement is given orally the Covered Entity shall document the statement including the agency's or official's identity and the suspension cannot be longer than 30 days.

B. Content of an Accounting

The Covered Entity shall provide the Individual with a written accounting that includes the disclosures of PHI that occurred during the past 6 years (or shorter period if requested by the Individual) prior to the date of the request for accounting, including disclosures to or by business associates of the Covered Entity. The accounting shall include the following for each disclosure:

1) Date of the disclosure;

2) Name of the entity or person who received the PHI and, if known, the address of such entity or person;

3) Brief description of the PHI disclosed; and

4) Brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for the disclosure.

---

the NPRM or whether HHS will scrap the proposed rules and publish a different set of rules on accounting of disclosures taking into account the large number of comments and concern about the current proposed rules. Until such time as final regulations on this topic are published, the Covered Entity's HIPAA policies will not include any changes on this topic from the HITECH Act.

[2] Covered Entity is not required to include in an Accounting of Disclosures, disclosures that were made incidental to another use or disclosure that is permissible under the Privacy Rule, however, to minimize incidental Disclosures, Covered Entity will take precautions to reasonably safeguard PHI as required by the Privacy Rule; and Disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the Disclosure.

If, during the period covered by the accounting, the Covered Entity has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide the information listed above for the first disclosure. In addition, the Covered Entity shall provide the frequency, periodicity or number of disclosures made during the accounting period and the date of the last such disclosure during the accounting period.

C. Provision of the Accounting

The Privacy Officer shall process all accounting requests. The Covered Entity shall act on the Individual's request for an accounting, no later than 60 days after the request is made, as follows:

1) Provide the Individual with an accounting; or

2) If the Covered Entity is unable to provide the accounting within the 60 days, the Covered Entity can extend the time to provide the accounting by no more than 30 days if the Covered Entity provides the Individual with a written statement with the reason for the delay and the date by which the Covered Entity shall provide the accounting. The Covered Entity may only have one extension per request for accounting.

The Covered Entity shall provide the first accounting to an Individual for any 12-month period without charge. The Covered Entity may impose a reasonable, cost-based, fee for subsequent requests for an accounting by the same Individual within the 12 month period, provided that the Covered Entity informs the Individual in advance of the fee and provides the Individual with an opportunity to withdraw or modify the request.

D. Electronic Health Records

If and to the extent Covered Entity uses or maintains an Electronic Health Record, as that term is defined in § 13400 of HITECH, with respect to PHI, Covered Entity shall respond to requests from Individuals for an accounting of Disclosures as described in § 13405(c) of HITECH if, and when required by § 13405(c) of HITECH.

E. Form of Request

Covered Entity shall require Individuals to direct requests for an accounting of PHI to Russell Wood who shall request that the Individual requesting access to PHI complete an appropriate form. His contact information is:

Russell Wood
russell.wood@cicsmhds.org
123 1st Ave SW, (PO Box58)
Hampton IA 50441
641-456-2128
Fax 641-456-2852

F. Documentation

The Covered Entity shall document and retain the documentation that includes the written accounting provided to the Individual and the titles of the person or offices responsible for receiving and processing requests for an accounting.

INSTRUCTIONS RELATED TO REQUESTS FOR ACCOUNTING

1) Provide the Individual with a Request for Accounting Form.
2) Provide the necessary disclosures to the Individual.
3) Retain documentation to be included in the Individual's designated record set.

SEE REQUEST FOR ACCOUNTING DISCLOSURE LOG FORM AND REQUEST FOR ACCOUNTING FORM ATTACHED TO THIS HIPAA MANUAL

ACCOUNTING DISCLOSURE LOG

Individual Name: _____ Individual Number: _____

Date request received	Person making request	Date of Disclosure	Name and Address of Recipient of PHI	Description of PHI disclosed	Purpose of Disclosure (or copy of written request)	Name of Staff processing request

REQUEST FOR ACCOUNTING OF DISCLOSURES

Name: (First/Middle/Last) _____
Address: (Street/City/Sate/Zip code) _____

_____

Date of Birth: _____ Social Security number: _____
Date of Request:

I REQUEST AN ACCOUNTING OF ALL DISCLOSURES FOR THE FOLLOWING TIME PERIOD: *(note: the maximum time period that can be requested is six years prior to the date of your request but not for time periods prior to April 14, 2003):*

From: (Month/Day/Year) _____ to: (Month/Day/Year) _____

I REQUEST THE ACCOUNTING BE SENT TO THE FOLLOWING ADDRESS:

_____

_____

I understand that there is no charge for the first accounting request in a 12-month period. For subsequent requests in the same 12-month period, the charge is $.50 per page.

I UNDERSTAND THE FOLLOWING: (check one)

_____ there is no fee for this request
_____ there is a fee for this request

I UNDERSTAND THE ACCOUNTING I HAVE REQUESTED WILL BE PROVIDED TO ME WITHIN 60 DAYS OF THIS REQUEST UNLESS I AM NOTIFIED IN WRITING THAT AN EXTENSION OF UP TO 30 DAYS IS NEEDED.

_____

Signature of Individual Date

IN THE EVENT THIS REQUEST IS MADE BY THE INDIVIDUAL'S PERSONAL REPRESENTATIVE:

_____

Signature of Personal Representative Date

_____

Legal Authority of the Personal Representative

For Covered Entity Use:

Date request received: _____ Date accounting sent: _____
Extension requested: ____ No ____ Yes - If yes, give reason: _____
_____ Individual notified in writing of extension
Name of Individual processing request:

AMENDING PHI POLICY

I. POLICY

Covered Entity recognizes that Individual rights are a critical component to maintaining quality care and service, and is committed to allowing Individuals to exercise their rights under applicable federal, state and/or local laws and regulations. To support this commitment, Covered Entity will maintain written Policies and Procedures to provide guidance when faced with a request by an Individual to amend his or her PHI.

II. PURPOSE

The purpose of this policy is to provide Individuals with the right to amend PHI when such amendment is required and appropriate.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.526

IV. PROCEDURE

A. General Rule

An Individual has the right to request that Covered Entity amend PHI about the Individual that is contained in a designated record set of Covered Entity, for as long as the PHI is maintained by the Covered Entity. However, the Covered Entity has the right under certain circumstances that are further described in this policy, to deny a request for amendment.

B. Form of Request

The Covered Entity shall require Individuals to direct requests for amendment of their PHI to Russell Wood, who shall request that the Individual requesting amendment to PHI complete an appropriate form. His contact information is:

Russell Wood
russell.wood@cicsmhds.org
123 1st Ave SW, (PO Box58)
Hampton IA 50441
641-456-2128
Fax 641-456-2852

C. Accepting an Individual's Request for Amendment

If the Covered Entity has no grounds to deny the Individual's request for amendment, the Covered Entity must do all of the following:

1) Make the appropriate amendment to the Individual's PHI or record. The Covered Entity should, at a minimum, identify records that are affected by the amendment and append or otherwise provide a link to the location of the amendment.

2) Inform the Individual on a timely basis that the amendment is accepted and obtain the Individual's identification of an agreement to have Covered Entity notify the relevant persons with whom the amendment needs to be shared.

3) Make reasonable efforts to inform and provide the amendment within reasonable time to:

   a) persons identified by the Individual as having received PHI and needing the amendment; and
   b) persons, including business associates, that Covered Entity knows have the unamended information and may have relied, or might rely in the future, on the information to the detriment of the Individual.

D. Denying an Individual's Request for Amendment

Under certain circumstances, Covered Entity may deny the Individual's request for amendment to his or her PHI held by Covered Entity.

1) *Permissible Reasons for Denial*. Covered Entity may deny a request for amendment only for the following reasons:

   a) The PHI was not created by Covered Entity unless the Individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
   b) The PHI is not part of the Individual's Designated Record Set;
   c) the PHI would not be available for inspection under Covered Entity's policy regarding the Individual's right to access records; or
   d) The PHI is complete and accurate.

2) *Denial Procedures*. If Covered Entity denies the requested amendment, in whole or in part, Covered Entity must take the following steps.

   a) Covered Entity must provide the Individual with a valid, written denial that explains:

      i. the basis for the denial;
      ii. how the Individual may file a written statement disagreeing with the denial;
      iii. the Individual's option with respect to future disclosures of the disputed information; and
      iv. how the Individual may make a complaint to HHS.

   b) Covered Entity must permit the Individual to submit to Covered Entity a written statement disagreeing with the denial and the basis for the disagreement.
   c) Covered Entity may prepare a written rebuttal to the Individual's statement of disagreement. If Covered Entity prepares a rebuttal, it must provide a copy to the Individual.

d) Covered Entity must identify, as appropriate, the information in the Individual's record that is the subject of the disputed amendment and append or otherwise link to this information the request for an amendment, Covered Entity's denial of this request, the Individual's statement of disagreement, and Covered Entity's rebuttal to the information.

e) Covered Entity must adhere to the following guidelines if it makes future disclosures of the Individual's disputed PHI:

i. If the Individual has submitted a statement of disagreement, Covered Entity must include either the material appended to the record, or an accurate summary of it, with any subsequent disclosure of the PHI to which the disagreement relates.

ii. If the Individual has not submitted a written statement of disagreement, Covered Entity has to include the appended information with any subsequent disclosure only if the Individual has requested that Covered Entity do so.

E. Receiving a Notice of Amendment From Other Health Care Providers or Health Plans.

Other health care providers or health plans may contact Covered Entity to let it know that they have made amendments to the Individual's PHI. When Covered Entity is informed by another health care provider or health plan of an amendment to an Individual's PHI, Covered Entity must make necessary amendments to the PHI in its records. The notice of amendment should be retained by Covered Entity, with a copy forwarded to the Privacy Officer.

F. Time Period for Acting on Requests

Covered Entity must act on an Individual's request for an amendment within 60 days of the receipt of the request, including making the requested amendment or sending a written denial. When a request for amendment is received by Covered Entity, that request must be forwarded immediately to the Privacy Officer. If Covered Entity is unable to act on the request for amendment within 60 day, the Privacy Officer shall notify the Individual, within the initial 60 day time period, that it is extending the time for response by an additional 30 days, and provide the Individual with a written statement of the reasons for the delay and the date by which Covered Entity will complete its action on the request. The Covered Entity can only have one such extension per amendment request.

INSTRUCTIONS FOR RESPONDING TO A REQUEST FOR AMENDMENT

1) Have the Individual complete the Request for Amendment Form.
2) Explain to the Individual that the information will be reviewed and a decision will be made on whether the correction is accepted or denied.
3) If the amendment is accepted the PHI or designated record set shall be amended or appended with the requested amendment.
4) The Covered Entity shall notify others affected by the amendment, including business associates.
5) Explain the Individual's right to write a statement of disagreement for any denials and the Covered Entity's right to rebut the statement of disagreement.
6) Place the completed form in the Individual's designated record set and give a copy to the Individual.
7) The Covered Entity will retain the correction/amendment form for a period of 6 years.
8) Explain to the Individual that this information will accompany the designated record set anytime a request is made to release information.
9) If a statement of disagreement is filed pursuant to a Covered Entity denial, attach to the Individual's designated record set.
10) If a rebuttal statement is provided by the Covered Entity, attach to the Individual's designated record set.

SEE ATTACHED INDIVIDUAL'S REQUEST FOR AMENDMENT FORM

INDIVIDUAL'S REQUEST FOR AMENDMENT OF PHI

Name: (First/Middle/Last) _____
Address: (Street/City/Sate/Zip code) _____

_____

Date of Birth: _____ Social Security number: _____
Date of Request:
Date of entry to be amended:
Type of entry to be amended:
Please explain how the entry is incorrect or incomplete. What should the entry say to be more accurate or complete?

_____

Would you like this amendment sent to anyone to whom we may have disclosed the information in the past? If so, please specify the name and address of the organization or Individual.

_____

_____

I understand that the Covered Entity reserves the right to amend the PHI based on my request, and the original entry(ies) in the record will not be altered. This request to amend will be made a part of my permanent health care record.

_____

Signature of Individual Date

IN THE EVENT THIS REQUEST IS MADE BY THE INDIVIDUAL'S PERSONAL REPRESENTATIVE

_____

Signature of Personal Representative Date

_____

Legal Authority of Personal Representative

For Covered Entity Use:

Date Received_____ Accepted _____ Denied _____

If denied, check reason for denial:

_____PHI is accurate and complete
_____PHI was not created by the Covered Entity
_____PHI is not part of Individual's designated record set
_____Pursuant to federal law PHI is not available to Individual for inspection (e.g. psychotherapy notes)

_____ If denied, Individual was informed of denial in writing

_____ If accepted, Individual was informed of acceptance

Name/title of Individual processing this request: _____

REQUESTS FOR PRIVACY PROTECTION FOR PHI POLICY

V. POLICY

Covered Entity is committed to ensuring the confidentiality of PHI (PHI), and ensuring the rights of Individuals under HIPAA to request restrictions of uses and disclosures of their PHI and requests to receive communications of PHI by alternative means or at alternative locations.

VI. PURPOSE

To set out procedures for Covered Entity workforce to follow to enable Individuals to request restrictions on uses and disclosures of their PHI and to request alternative means of communication.

VII. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.522

VIII. PROCEDURE

A. Requesting Restrictions

The Covered Entity shall permit an Individual to request that the Covered Entity restrict:

1) Uses and disclosures of PHI about the Individual to carry out treatment, payment or health care operations; and

2) Disclosures made to family members or others pursuant to §164.510 under which the Covered Entity can generally disclose PHI to family members or others who are involved in the Individual's care or payment for care.

B. Covered Entity's Response to Requests for Restriction

1) General Rule. Except as set forth below, the Covered Entity is not required to agree to the requested restriction.

2) Voluntary Agreement to a Restriction. If the Covered Entity does agree to restrict PHI, the Covered Entity shall not use or disclose PHI in violation of such restriction, except if the restricted information is needed in an emergency situation. If restricted information is disclosed during an emergency situation, the Covered Entity shall request that the health care provider not further use or disclose the restricted information. The Covered Entity may not agree to a restriction on disclosure of PHI if the HIPAA privacy provisions require the disclosure.

3) Mandatory Agreement to a Restriction. A Covered Entity must agree to the request of an Individual to restrict disclosures of such Individual's PHI, if the disclosure is to a health plan for purposes of carrying out payment or healthcare operations (and is not for treatment purposes), and the PHI pertains solely to a healthcare item or service for which the Covered Entity was paid out of pocket in full.

C. Terminating a Restriction

The Covered Entity may terminate its agreement to a restriction, if:

1) the Individual agrees to or requests the termination in writing;

2) the Individual orally agrees to the termination and the oral agreement is documented; or

3) The Covered Entity informs the Individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the Individual, and the termination is not effective with respect to PHI that the Covered Entity is mandated to agree to restrict upon the Individual's request, as set out in this Policy, above.

D. Confidential Communications.

1) A Covered Entity that is a health care provider shall permit Individuals to request and shall accommodate reasonable requests by Individuals to receive communications of PHI from the Covered Entity by alternate means or at alternate locations. The Covered Entity cannot require an explanation from the Individual as to the basis for the request as a condition of providing communications on the confidential basis.

2) A Covered Entity that is a health plan shall permit Individuals to request and shall accommodate reasonable requests by Individuals to receive communications of PHI by alternate means and at alternate locations, if the Individual clearly states that the disclosure of all or part of that information could endanger the Individual.

3) Conditions on Providing Confidential Communications.

   a) The Covered Entity may require an Individual to a make a request for a confidential communication in writing.
   b) The Covered Entity may condition the provision of a reasonable accommodation on:

      i. When appropriate, information on how payment, if any, will be handled; and
      ii. Specification of an alternate address or other method of contact.

INSTRUCTIONS RELATED TO ASSISTING INDIVIDUALS IN REQUESTING RESTRICTIONS AND CONFIDENTIAL COMMUNICATIONS

1. Provide the Individual with appropriate forms.

2. If reasonable, change communications to alternate means or location.

3. Retain documentation to be included in the Individual's designated record set.

SEE ATTACHED REQUEST FORM FOR INDIVIDUALS TO COMPLETE WHEN REQUESTING CONFIDENTIAL COMMUNICATIONS

REQUEST FOR ALTERNATIVE MEANS OR LOCATION OF CONFIDENTIAL COMMUNICATIONS

Name: (First/Middle/Last) _____
Address: (Street/City/Sate/Zip code) _____

_____

Date of Birth: _____ Social Security number: _____
Date of Request:

I REQUEST THE COVERED ENTITY TO COMMUNICATE CONFIDENTIAL INFORMATION TO ME IN THE FOLLOWING MANNER:

☐ Telephone communication at the following telephone number: _____
_____ Leave a message on an answering machine at this number
_____ do not leave a message on an answering machine at this number

☐ Written communication to be mailed to the following address:

_____

☐ Other: _____

I further understand that the Covered Entity may condition its acceptance of these conditions upon how payment for services will be made or upon my providing an alternative address or other method of contact.

_____
Signature of Individual Date

IN THE EVENT THIS REQUEST IS MADE BY THE INDIVIDUAL'S PERSONAL REPRESENTATIVE

_____
Signature of Personal Representative Date

_____

_____
Legal authority of Personal Representative

For Covered Entity Use:

_____ Accept request for alternative communication

_____ Reject request for alternative communication. Reason rejected: _____

Name/Title of Individual processing this request: _____
Date request processed:

AUTHORIZATIONS POLICY

I. POLICY

The Covered Entity requires an Authorization to Release form be completed for all Uses and Disclosures of PHI, other than those required by law, for treatment, payment and health care operations, or as otherwise permitted without an Authorization, except for disclosure that are prohibited under law.

For any disclosures of Mental Health Information, or other information that is provided greater protection under Iowa law, the Covered Entity requires specific processes be followed in order to comply with these Iowa laws that are more restrictive than HIPAA. See the Iowa Laws Providing Greater Protection Policy for further information.

II. PURPOSE

The purpose of this Authorizations Policy is to give workforce members guidance about the circumstances under which an Authorization must be obtained and the process to obtain an Authorization, in order to comply with the Health Insurance Portability and Accountability Act (HIPAA) and with Iowa's Mental Health Privacy law.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.502(a)
- 45 C.F.R. §164.508
- Iowa Code §228.2
- Iowa Code §228.3
- Iowa Laws Providing Greater Protection Disclosures Policy
- Overview: Handling Uses and Disclosures of Protected Health Information
- Family, Friend Involvement/Personal Representatives and Deceased Individual Policy
- Health Oversight Uses and Disclosures Policy
- Judicial and Administrative Purposes Disclosures Policy
- Law Enforcement Disclosures Policy
- Limited Data Set Policy
- Marketing Policy
- Minimum Necessary Policy
- Required By Law Disclosures Policy
- Research Disclosures Policy
- Averting Serious Threat Disclosures Policy
- Specialized Government Functions Use and Disclosures Policy

IV. PROCEDURE

A. General Rule for Uses and Disclosures of PHI that is Not Mental Health Information (as defined under Iowa Law).

Covered Entity shall obtain a signed Authorization form (attached) from all Individuals before Using or Disclosing PHI for purposes other than treatment, payment or health care operations or

unless the Use or Disclosure is otherwise permitted, required or prohibited under HIPAA or this Policy Manual.

B. General Rule for Uses and Disclosures of Mental Health Information (as Defined under Iowa Law)

Mental Health Information is defined as oral, written, or recorded information which indicates the identity of an Individual receiving professional services and which relates to the diagnosis, course, or treatment of the Individual's mental or emotional condition. Covered Entity shall not disclose Mental Health Information except as set out in this policy and in compliance with Iowa law regarding the disclosure of Mental Health Information. See the Iowa Laws Providing Greater Protection Policy for further information.

C. Restriction on Conditioning Treatment on Authorization

The Covered Entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits, if applicable, on the provision of an Authorization except that the Covered Entity may condition enrollment or eligibility for benefits on the provision of an authorization requested by the Covered Entity prior to the Individual's enrollment in the health plan:

1) If the authorization is sought for the eligibility or enrollment determinations relating to the Individual; or

2) For its underwriting or risk rating determinations, and

The authorization is not for a use or disclosure of psychotherapy notes.

D. Authorization Rules Related to Psychotherapy Notes

Prior to any Use or Disclosure of psychotherapy notes, including for treatment, payment or health care operations, Covered Entity shall obtain an Authorization from the Individual, except if the Use or Disclosure is for:

1) The following uses to carry out treatment, payment or health care operations:

   a) The treatment activities of the originator of the psychotherapy notes;
   b) The Covered Entity's own training programs in which mental health students, trainees or practitioners practice, under supervision, their skills in counseling; or
   c) Covered Entity's defense in a legal action or other proceeding brought by the Individual.

2) A Use or Disclosure of psychotherapy notes that is required or permitted under HIPAA and applicable state law.

An authorization for a use or disclosure of psychotherapy notes may not be combined with another authorization for the disclosure of other PHI, but may be combined with another authorization for a use or disclosure of the same Individual's psychotherapy notes.

E. Authorization Needed for Marketing use of PHI

Covered Entity shall obtain an Individual's Authorization prior to any Use or Disclosure for marketing purposes. Refer to the Marketing Policy for further details on the restrictions of the use of PHI for marketing purposes.

F. Authorization Needed for Sale of PHI

Covered Entity shall obtain an Individual's Authorization prior to receiving any direct or indirect payment in exchange for PHI. Refer to the Sale of PHI Policy for further details on the restrictions related to the sale of PHI.

G. Circumstances Under Which No Authorization is Required

With the exception of Mental Health Information and other information that is afforded greater protection under Iowa law, the Covered Entity is not required to obtain Authorization for the following purposes (which are described in greater detail in the Overview, and in the applicable policies in this Privacy Manual):

1) To carry out treatment, payment or health care operations;

2) Uses and Disclosures required by law;

3) Uses and Disclosures for public health activities;

4) Disclosures about victims of abuse, neglect or domestic violence;

5) Uses and Disclosures for health oversight activities;

6) Disclosures for judicial and administrative proceedings;

7) Disclosures for law enforcement purposes;

8) Disclosing PHI about decedents;

9) Uses and Disclosures for cadaveric organ, eye or tissue donation purposes;

10) Uses and Disclosures for research purposes;

11) Uses and Disclosures to avert a serious threat to health or safety;

12) Uses and Disclosures for specialized government functions; and

13) Disclosures for workers' compensation.

Iowa's Mental Health Privacy Law is very restrictive regarding disclosures of mental health information without a signed voluntary authorization from the Individual or the Individual's legal representative. Contact the Privacy Officer any time that a request is made to disclose mental health information without a signed authorization form. Additionally, review the Iowa Laws Providing Greater Protections Policy for further information on additional protections under Iowa law for various information.

H. Core Elements for Authorizations

An Authorization will contain the following core elements (note that a Mental Health Authorization must have additional elements, as listed below):

1) Specific and meaningful description of the information to be used or disclosed;

2) Name or other specific identification of the person(s) or class of persons, authorized to make the requested use or disclosure;

3) Name or other specific identification of the person(s), or class of persons, to whom the Covered Entity may make the requested use or disclosure;

4) A description of each purpose of the requested use or disclosure. The statement "at the request of the Individual" is a sufficient description of the purpose when an Individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;

5) An expiration date or expiration event that relates to the Individual for the purpose of the use or disclosure;

6) Signature of the Individual and date. If the Individual's personal representative signs the authorization, a description of the representative's authority to act for the Individual must be provided.

In addition to the above core elements, the authorization shall also contain the following statements that adequately put the Individual on notice:

1) the Individual's right to revoke the authorization in writing;

2) the exceptions to the right to revoke or a reference to the Covered Entity's Notice of Privacy Practices;

3) the ability of the Covered Entity to condition treatment, payment, enrollment and/or eligibility for benefits on the authorization by stating the consequences to the Individual of a refusal to sign the authorization; and

4) The potential for information disclosed to be subject to re-disclosure by the recipient.

Further, the authorization will be written in plain language and a copy of the signed authorization must be given to the Individual.

I. Additional Elements for Disclosures of Mental Health Information

The following additional rules apply to disclosures of Mental Health Information:

An Individual eighteen years of age or older, or an Individual's legal representative, may consent to the disclosure of mental health information relating to the Individual by signing an authorization form. The authorization shall:

1) Specify the nature of the mental health information to be disclosed;

2) State the persons or type of persons authorized to disclose the information;

3) State the purposes for which the information may be used both at the time of the disclosure and in the future;

4) Advise the Individual of the Individual's right to inspect the disclosed mental health information at any time;

5) State that the authorization is subject to revocation and state the conditions of revocation;

6) Specify the length of time for which the authorization is valid; and

7) Contain the date on which the authorization was signed.

A copy of the authorization shall be provided to the Individual or to the legal representative of the Individual authorizing the disclosure, and must be included in the Individual's record of mental health information.

Upon the disclosure of mental health information for any reason, the person disclosing the mental health information shall enter a notation on and maintain the notation with the Individual's record of mental health information, stating the date of the disclosure and the name of the recipient of mental health information.

Further, the person disclosing the mental health information shall give the recipient of the information a statement which informs the recipient that disclosures may only be made pursuant to the written authorization of an Individual or an Individual's legal representative, or as otherwise provided under state and federal law, that the unauthorized disclosure of mental health information is unlawful, and that civil damages and criminal penalties may be applicable to the unauthorized disclosure of mental health information.

A recipient of mental health information shall not disclose the information received, except as specifically authorized for initial disclosure. However, mental health information may be transferred at any time to another facility, physician, or mental health professional in cases of a medical emergency or if the Individual or the Individual's legal representative requests the transfer in writing for the purposes of receipt of medical or mental health professional services, at which time the requirements of this policy regarding the disclosure of mental health information shall be followed.

An Individual or an Individual's legal representative may revoke a prior authorization by providing a written revocation to the recipient named in the authorization and to the Individual/entity previously authorized to disclose the mental health information. The revocation is effective upon receipt of the written revocation by the person previously authorized to disclose the mental health information. After the effective revocation date, mental health information shall not be disclosed pursuant to the revoked authorization. However, mental health information previously disclosed pursuant to the revoked authorization may be used for the purposes stated in the original written authorization.

J. Defective Authorization

An authorization will not be valid if it passes the expiration date; if it has not been filled out completely; if revoked or if any material information is known by the Covered Entity to be false. In addition, the Covered Entity will not combine authorizations for psychotherapy notes with any other document to create a compound authorization.

K. Revocation of Authorization

An Individual may revoke an authorization at any time, provided that the revocation is in writing, except, to the extent that:

1) The Covered Entity has taken action in reliance on the authorization, or

2) The authorization was a condition of obtaining insurance coverage.

L. Record Retention

The Covered Entity will document and retain any signed authorization for a period of six (6) years.

INSTRUCTIONS FOR USING/DISCLOSING PHI AND FOR AUTHORIZATIONS

1) Determine if an authorization is required to disclose the PHI.
2) Contact the Privacy Officer if you have any questions about whether an authorization is required; especially if a request is made for the disclosure of mental health information without a signed authorization.
3) Review the purpose of the authorization with the Individual.
4) Ask the Individual to read, complete, sign and date the authorization.
5) Explain to the Individual that the authorization can be revoked, in writing, at any time, the exceptions to revocation and the consequence of the revocation.
6) Explain to the Individual that they have the right to not sign the authorization and the consequences of not signing the authorization.
7) Give a signed copy of the authorization to the Individual.
8) Give the Individual a copy of the County's Notice of Privacy Practices if they have not already received one.
9) Place the completed authorization in the Individual's records.

SEE AUTHORIZATION FORM ATTACHED TO THIS HIPAA MANUAL

AUTHORIZATION FOR DISCLOSURE OF PHI

Please complete this form in its entirety. This authorization is not valid and the Covered Entity will not release your PHI unless the form is completed in its entirety. A copy of the signed authorization will be provided to you.

THE FOLLOWING PERSON(S) OR ENTITY:
Name of Person(s) or Entity: _____

Address of Person(s) or Entity: _____
_____

SHALL DISCLOSE THE FOLLOWING INFORMATION FROM THE HEALTH RECORDS OF:
Name: (First/Middle/Last) _____
Address: (Street/City/ State/Zip code) _____
Birth date: (Month/Day/Year) _____Social Security #: _____
Telephone Number: (Home) _____ (Work) _____

THIS INFORMATION SHALL BE DISCLOSED TO THE FOLLOWING PERSON(S) OR ENTITY:
Name of Person(s) or Entity:_____
Address of Person(s) or Entity:_____

THE INFORMATION DISCLOSED SHALL COVER HEALTH CARE FOR THE FOLLOWING PERIOD(S) OF TIME:

From: (month/date/year) _____To: (month/date/year) _____
From: (month/date/year) _____To: (month/date/year) _____

THE INFORMATION SHALL BE DISCLOSED FOR THE FOLLOWING PURPOSE(S):
(Not required if the disclosure is requested by the Individual)
_____
_____

THE FOLLOWING INFORMATION SHALL BE RELEASED:
_____
_____

I UNDERSTAND THAT THIS WILL INCLUDE INFORMATION RELATING TO: (Initial, if applicable)

_____ Acquired Immunodeficiency Syndrome (AIDS) and/or Human Immunodeficiency Virus (HIV).

_____ Behavioral/Mental Health service/psychiatric care. (Note: you have the right to inspect the disclosed mental health information at any time)

_____ Treatment for alcohol and/or drug abuse.

AFFIRMATION OF AUTHORIZATION:

I give the person(s) or entity named above permission to disclose only the information I have identified on this authorization form to the person(s) or entity I have named and only for the purposes I have identified. I understand: (*Please initial after reading each statement*)

_____ This authorization is valid for one year from the date I sign unless revoked prior to that date.

_____ I may refuse to sign this authorization (A refusal to sign the authorization may affect payment for or eligibility for benefits).

_____ I may revoke this authorization in writing at any time. (A revocation of this authorization may affect payment for or eligibility for benefits). This authorization cannot be revoked to the extent that the Covered Entity has taken action in reliance on the authorization or the authorization was a condition of obtaining insurance coverage.

_____ I understand that this information may be re-disclosed by the person(s) or entity receiving the information and no longer protected by 45 C.F.R. §164.508.

I may access my PHI by following the procedure outlined in the Notice of Privacy Practices.

_____

Signature of the Individual Date

IN THE EVENT THIS REQUEST IS MADE BY THE INDIVIDUAL'S PERSONAL REPRESENTATIVE

_____

Signature of personal representative Date

_____

Legal authority of personal representative

The following statement pertains to any disclosure or redisclosure of substance abuse, alcohol or drug treatment information, mental health information, or HIV/AIDS-related information:

This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR Part 2), or Iowa confidentiality rules (Iowa Code §228, Iowa Code §141A). The law prohibits you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by Iowa Code §228, Iowa Code §141A or 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the records protected by Federal confidentiality rules (42 CFR Part 2) to criminally investigate or prosecute any alcohol or drug abuse patient.

A COPY OF THIS SIGNED AUTHORIZATION MUST BE GIVEN TO THE PATIENT OR PATIENT'S REPRESENTATIVE. NOTE: PHOTOCOPY OF THIS SIGNED AUTHORIZATION SHALL BE AS EFFECTIVE AS THE ORIGINAL.

FAMILY, FRIEND INVOLVEMENT/PERSONAL REPRESENTATIVES AND DECEASED INDIVIDUAL POLICY

I. POLICY

When Covered Entity provides services to Individuals, employees may receive inquiries from Individuals, family members, friends or personal representatives to disclose a particular Individual's PHI for various purposes. To comply with the provisions of HIPAA, employees will ensure that appropriate steps are taken to verify the identity and authority of Individuals and entities requesting PHI, as required by the Privacy Rule and other federal, state and/or local laws and regulations.

II. PURPOSE

This Policy provides guidance to employees on handling inquiries from family members, friends or personal representatives in a manner that complies with the requirements of the Privacy Rule.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.510(b)
- 45 C.F.R. §164.502(g)

IV. PROCEDURE

A. Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes

In accordance with the following procedures, Covered Entity may disclose to an Individual's family member, close personal friend or any other person identified by the Individual only the PHI that is directly related to that person's involvement in the Individual's care or payment for care. Further, in accordance with the following procedures, Covered Entity may disclose to a family member, a personal representative of the Individual, or another person responsible for the care of the Individual, PHI to notify or assist in notifying (including identifying or locating) such family, friend or personal representative of the Individual's location, general condition, or death.

1) *Individual Present and Has Capacity*. If the Individual is present for, or otherwise available prior to, a use or disclosure permitted under this section, and has the capacity to make health care decisions, the Covered Entity may use or disclose the PHI to the Individuals described above if the Covered Entity:

   a) Obtains the Individual's agreement;
   b) Provides the Individual with an opportunity to object and the Individual does not express an objection to the disclosure; or
   c) Reasonably infer from the circumstances, based on the exercise of professional judgment, that the Individual does not object to the disclosure.

2) *Individual Not Present or Lacks Capacity*. If the Individual is not present or the Individual lacks capacity to consent (due to an emergency condition or otherwise), the Covered Entity may, in the exercise of professional judgment, determine whether

the disclosure is in the best interests of the Individual, and, if so, disclose only the PHI that is directly relevant to the person's involvement with the Individual's care or payment related to the Individual's care or needed for notification purposes. A Covered Entity may use professional judgment and its experience with common practice to make reasonable inferences of the Individual's best interests in allowing a person to act on behalf of the Individual to pick up certain medical records or discuss billing or payment matters.

3) *Deceased Individual*. If the Individual is deceased, a Covered Entity may disclose to the persons identified above who were involved in the Individual's care or payment for health care prior to the Individual's death, PHI of the Individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the Individual that is known to the Covered Entity.

4) *Disaster Relief*. A Covered Entity may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted under this section.

B. Family Members. With the exception of the circumstances described above, if the Covered Entity receives an inquiry from a family member regarding an Individual's PHI, the Covered Entity shall inform the Individual that the Individual must authorize the disclosure. The employee may then forward an Authorization form to the Individual.

C. Personal Representatives

1) General Rules. Except as provided in Paragraphs 2 and 3 below, the personal representative of an Individual shall have the same rights as the Individual and shall be treated as the Individual for purposes of Covered Entity's Policies and Procedures and the Privacy Rules.

   a) A person who has authority to make health care related decisions on behalf of another adult or emancipated minor shall be treated as a personal representative of such Individual.
   b) An executor, administrator or other person authorized to act on behalf of a deceased Individual or the Individual's estate shall be treated as a personal representative of such Individual.
   c) If an employee questions, to any extent, whether a person is a personal representative of an Individual, the Privacy Officer should be consulted.

2) Abuse, Neglect and Endangerment. Covered Entity may elect not to treat a person as a personal representative of an Individual if there is a reasonable basis for believing that the Individual has been or may be the subject of domestic violence, abuse or neglect by such person or treating such person as the personal representative may endanger the Individual. If abuse, neglect or endangerment is suspected, an employee shall immediately consult with the Privacy Officer for a determination as to whether or not to treat the person as a personal representative of the Individual.

3) Minor Children.

a) Payment Purposes. For purposes of payment, the parent, guardian or other person acting in a parental capacity (e.g., foster parent or step-parent) (collectively referred to herein as "Parent") shall be authorized to act and shall be treated as the personal representative of an unemancipated minor child.

b) All other Purposes. For all other purposes, unless applicable state law (including case law) specifically permits or prohibits disclosure to or access by the Parent to the PHI of such minor child, a Parent shall be authorized to act and shall be treated as the personal representative of an unemancipated minor child under Covered Entity's Policies and Procedures, except to the extent that:

i. the minor has consented to the health care, no other consent is required by law, and the minor has not requested that the Parent be treated as a personal representative;

ii. the minor child may lawfully consent to the health care provided without the consent of a Parent and the minor (or a court or other legally authorized person) has provided such consent; or

iii. the Parent assents to an agreement of confidentiality.

For purposes other than Payment, an employee shall consult immediately with the Privacy Officer with respect to whether a Parent will be treated as the personal representative of an unemancipated minor.

HEALTH OVERSIGHT USES AND DISCLOSURES POLICY

I. POLICY

For most disclosures other than in the usual course of treatment, payment, or health care operations, Covered Entity must obtain the Individual's Authorization before using or disclosing the Individual's PHI. However, Covered Entity may use or disclose PHI without an Authorization, for health oversight activities pursuant to the Privacy Rule.

II. PURPOSE

The purpose of this policy is to provide guidance and to ensure that any use or disclosure of PHI for health oversight activities is in compliance with all applicable laws and regulations.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.512(d)

IV. PROCEDURE

A. Health Oversight Agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

B. General Rule Regarding Use or Disclosure of PHI for Purposes Other Than Treatment, Payment or Health Care Operations. Under the Privacy Rule, Covered Entity may not disclose an Individual's PHI for purposes other than treatment, payment or health care operations or other permitted uses and disclosures, without obtaining the Individual's prior written Authorization.

C. Exceptions to General Rule. In some situations, Covered Entity may have an obligation to disclose PHI to a Health Oversight Agency, if the conditions set forth in this Policy are met prior to the use or disclosure. In these circumstances, PHI may be disclosed without obtaining the written Authorization of the Individual, and without providing the opportunity for the Individual to agree or object.

D. General Requirements for Use or Disclosure of PHI to a Health Oversight Agency. From time to time, a Health Oversight Agency will request PHI from Covered Entity. Covered Entity may disclose PHI for health oversight activities in accordance with the following guidelines:

1) Covered Entity may disclose PHI to a Health Oversight Agency for health oversight activities including:

a) audits;
b) civil, administrative or criminal investigations;
c) inspections;
d) licensure or disciplinary actions;
e) civil, administrative or criminal proceedings; or
f) other activities necessary for appropriate oversight of the following:

i. the health care system;
ii. government benefit programs for which health information is relevant to beneficiary eligibility;
iii. entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards;
iv. entities subject to civil rights laws for which health information is necessary for determining compliance.

2) If a health oversight activity or investigation is conducted in conjunction with an oversight or investigation relating to a claim for public benefits unrelated to health, Covered Entity considers the joint activity to be a health oversight activity and will disclose PHI.

3) Covered Entity shall not disclose PHI without an Authorization in cases where an Individual is the subject of an investigation or other activity, if such investigation or other activity does not arise out of and is not directly related to:

a) The receipt of health care;
b) A claim for public benefits related to health; or
c) Qualification for or receipt of public benefits or services when an Individual's health is integral to the claim for public benefits or services.

E. Privacy Officer. When Covered Entity is presented with a request for PHI from a Health Oversight Agency, the employee will confer with the Privacy Officer prior to making any such use or disclosure. The Privacy Officer will evaluate the proposed use or disclosure. No Covered Entity employee may make such a use or disclosure prior to conferring with the Privacy Officer. At times, state law may prohibit such disclosure even though it would otherwise be permitted under HIPAA (e.g., disclosure of Mental Health Information- See the Iowa Laws Providing Greater Protection Policy).

F. Response to a Request for Disclosure From a Health Oversight Agency. Covered Entity personnel will confer with the Privacy Officer and shall follow the following guidelines:

1) Covered Entity personnel will follow appropriate policies and procedures for verifying the identity and authority of Individuals requesting PHI. See separate Policy, "Verification".

2) If the identity and authority of the Individual requesting access to PHI cannot be verified, Covered Entity personnel will refer the issue to the Privacy Officer for immediate action.

3) Once the request for access and the verification of the Health Oversight Agency representative's identity and authority have been verified, a decision will be made whether or not the disclosure is appropriate and may be made. Once it is determined that use or disclosure is appropriate, Covered Entity personnel with appropriate access clearance will access the Individual's PHI using proper access procedures.

4) The requested PHI will be delivered to the Health Oversight Agency requesting it in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.

5) The Privacy Officer will appropriately document the request and delivery of the PHI.

JUDICIAL OR ADMINISTRATIVE PURPOSES DISCLOSURES POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individuals' PHI. For most disclosures other than in the usual course of treatment, payment, or health care operations Covered Entity must obtain the Individual's Authorization before using or disclosing the Individual's PHI.

II. PURPOSE

The purpose of this policy is to provide Individuals with guidance about Covered Entity's rights and obligations in response to a request for access to PHI through the judicial or an administrative process.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.512(e)

IV. PROCEDURE

A. General Rule Regarding Use or Disclosure of PHI for Purposes Other Than Treatment, Payment or Health Care Operations. Under the Privacy Rule, Covered Entity may not disclose an Individual's PHI for purposes other than treatment, payment or health care operations or other permitted uses and disclosures without the Individual's prior written Authorization.

B. Exceptions to General Rule. In some situations, PHI may be disclosed pursuant to a judicial or administrative process without obtaining written Authorization of the Individual, or the opportunity for the Individual to agree or object. From time to time, Covered Entity may receive a request to disclose PHI through a court order or an order from an administrative tribunal. In such a situation, the Privacy Officer must be immediately notified.

C. General Requirements for Judicial and Administrative Release. Covered Entity shall comply with all lawful and appropriate requests from regulatory and judicial authorities and disclose PHI necessary to respond to a subpoena, grand jury subpoena, discovery request, or other lawful process, whether or not accompanied by the order of a court or administrative tribunal. Only the information that is responsive to the request may be disclosed.

D. Receipt of a Request for PHI from a Judicial Or Administrative Tribunal. When a Covered Entity employee is in receipt of a request for PHI pursuant to a judicial or administrative process, the employee must immediately forward the request to the Privacy Officer. The Privacy Officer will evaluate the request, in consultation with legal counsel. No Covered Entity employee, regardless of title and/or position is authorized to respond to such a request or to release information prior to forwarding the request on to the Privacy Officer.

E. Response to Request for PHI from a Judicial or Administrative Tribunal. Upon receipt of a request for PHI from a judicial or administrative tribunal, the Privacy Officer shall consult legal counsel. PHI may only be released in such a situation where either of the following have occurred:

1) Covered Entity has received satisfactory assurances from the party seeking the information that reasonable efforts have been made by such party to ensure that the Individual who is the subject of the PHI that has been requested has been given notice of the request, which meets certain requirements as follows; or

   a) Covered Entity shall obtain a written statement and accompanying documentation from the requestor, demonstrating that a notice has been given to the Individual, which contained sufficient information about the litigation or proceeding in which the PHI is requested to permit the Individual to raise an objection to the court or administrative tribunal.

   b) In the event that reasonable efforts have been made to ensure that the Individual was given notice of the request, Covered Entity shall obtain from the requesting party a written statement and accompanying documentation that:

      i. time for raising objections to the court or administrative tribunal has elapsed; and
      ii. no objections were filed; or
      iii. the court has resolved all objections filed by the Individual or the administrative tribunal and the disclosures being sought are consistent with such resolution.

2) Covered entity received satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets certain requirements as follow:

   a) Where reasonable efforts have been made to secure a qualified protective order, Covered Entity shall obtain from the requesting party a written statement and accompanying documentation demonstrating that:

      i. the parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
      ii. the party seeking the PHI has requested a qualified protective order from such a court or administrative tribunal.

F. Verification. Covered Entity will follow Policies and Procedures for verifying the identity and authority of Individuals requesting PHI. No PHI shall be released in the absence of proper verification. See separate Policy and Procedure entitled “Verification of Identity”.

G. Once it is determined that disclosure is appropriate, the Privacy Officer will access the PHI and shall deliver it to the Individual in a secure and confidential manner.

LAW ENFORCEMENT DISCLOSURES POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individuals' PHI. For most disclosures other than in the usual course of treatment, payment, or health care operations, Covered Entity must obtain the Individual's Authorization before using or disclosing the Individual's PHI. However, pursuant to a law enforcement process, and subject to the requirements set forth in this Policy, PHI may be disclosed without the Authorization of the Individual, or the opportunity for the Individual to agree or object.

II. PURPOSE

The purpose of this policy is to provide guidance and to ensure that any use or disclosure of PHI for law enforcement purposes is in compliance with all applicable laws and regulations.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.512(f)

IV. PROCEDURE

A. Definition

Law Enforcement Official means an officer or employee or any agency or authority of the United States, a State, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law.

B. General Rule Regarding Use or Disclosure of PHI for Purposes Other Than Treatment, Payment or Health Care Operations. Under the Privacy Rule, Covered Entity may not disclose an Individual's PHI for purposes other than treatment, payment or health care operations without prior obtaining the Individual's Authorization.

C. Exceptions to General Rule. In some situations, Covered Entity may have an obligation to disclose PHI to a Law Enforcement Official, if the conditions set forth in this Policy are met prior to the use or disclosure. In these circumstances, PHI may be disclosed without obtaining the written Authorization of the Individual, and without providing the opportunity for the Individual to agree or object.

D. General Requirements for Use or Disclosure of PHI for Law Enforcement Purposes. From time to time, a law enforcement agency or Law Enforcement Official may request PHI. Covered Entity's legal counsel should to be immediately consulted in connection with such a request.

1) *Mandatory Reporting of Wounds of Other Injuries*. Covered Entity may disclose PHI as required by law, such as laws that require the reporting of criminal wounds or other physical injuries.

2) *Limited Disclosures*. Covered Entity may disclose PHI to a Law Enforcement Official in compliance with and as limited by the following conditions:

a) Covered Entity may disclose PHI without Individual Authorization in compliance with and as limited by the relevant requirements of a court order, court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena;

b) Covered Entity may disclose requested PHI pursuant to an administrative request made by a Law Enforcement Official, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, under the following conditions:

i. Covered Entity determines, in conjunction with the requesting party, that the information sought is relevant and material to a legitimate law enforcement inquiry;

ii. Covered Entity determines, in conjunction with the requesting party, that the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

iii. Covered Entity determines, in conjunction with the requesting party, that de-identified information could not reasonably be used.

3) *Identification and Location Purposes*. Other than stated in this Policy, Covered Entity shall not disclose PHI related to an Individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissues in response to a Law Enforcement Official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. However, Covered Entity may disclose the following PHI in response to a Law Enforcement Official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person:

a) name and address;
b) date and place of birth;
c) social security number;
d) ABO blood type and rh factor;
e) type of injury;
f) date and time of treatment;
g) date and time of death, if applicable; and
h) a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.

4) *Crime on the Premises*. Covered Entity may disclose to a Law Enforcement Official PHI that Covered Entity believes in good faith constitutes evidence of criminal conduct that occurred in the premises of Covered Entity.

5) *Reporting Crime in Emergencies*. Covered Entity may, in providing emergency health care in response to a medical emergency, other than emergency care provided

on the premises of Covered Entity, disclose PHI to a Law Enforcement Official if such disclosure appears necessary to alert law enforcement to:

a) The commission and nature of a crime;
b) The location of such crime or of the victim(s) of such crime; and
c) The identity, description, and location of the perpetrator of such crime.

6) *Reporting Regarding Decedents*. Covered Entity may disclose PHI about an Individual who has died to a Law Enforcement Official for the purpose of alerting law enforcement of the death of the Individual if Covered Entity has a suspicion that such death may have resulted from criminal conduct.

7) *Reporting Regarding Victims of Crime*. Covered Entity may disclose PHI in response to a Law Enforcement Official's request for such information about an Individual who is or is suspected to be a victim of a crime if the Individual agrees to the disclosure.

a) In cases where the Individual is suspected to be a victim of a crime and where Covered Entity is unable to obtain the Individual's agreement because of incapacity or other emergency circumstance, Covered Entity will:

i. Obtain representation from the requesting Law Enforcement Official that such information is needed to determine whether a violation of law by a person other than the victim occurred and that such information is not intended to be used against the victim;
ii. Obtain representation from the Law Enforcement Official that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the Individual is able to agree to the disclosure; and
iii. In the exercise of professional judgment, make a determination that the disclosure is in the best interest of the Individual before disclosing the PHI.

E. Privacy Officer. When a Covered Entity employee is presented with a request for PHI from a Law Enforcement Official, the employee will confer with the Privacy Officer, prior to making any such use or disclosure. The Privacy Officer will evaluate the proposed use or disclosure. No Covered Entity employee may make such a use or disclosure prior to conferring with the Privacy Officer.

F. Response to a Request to Disclosure From a Law Enforcement Official. Covered Entity personnel will confer with the Privacy Officer after verifying the identity and authority of the Law Enforcement Official and shall follow the following guidelines:

1) Covered Entity personnel will follow appropriate policies and procedures for verifying the identity and authority of Individuals requesting PHI. See separate Policy, "Verification of Identity".

2) If the identity and authority of the Individual requesting access to PHI cannot be verified, Covered Entity personnel will refer the issue to the Privacy Officer for immediate action.

3) Once the request for access and the verification of the Law Enforcement Official's identity and authority have been forwarded to the Privacy Officer, a decision will be made whether or not the disclosure is appropriate and may be made. Once it is determined that use or disclosure is appropriate, Covered Entity personnel with appropriate access clearance will access the Individual's PHI using proper access procedures.

4) The requested PHI will be delivered to the Law Enforcement Official requesting it in a secure and confidential manner such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.

5) The Privacy Officer will appropriately document the request and delivery of the PHI.

REQUIRED BY LAW DISCLOSURES POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individuals' PHI. For most disclosures other than in the usual course of treatment, payment, or health care operations, Covered Entity must obtain the Individual's Authorization before using or disclosing the Individual's PHI. On occasion, however, Covered Entity makes disclosures of PHI, without an Authorization when Covered Entity is required by law to do so.

II. PURPOSE

The purpose of this policy is to provide employees with guidance about Covered Entity's rights and obligations in disclosing PHI in response to various obligations under federal, state and local law.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.512(a)

IV. PROCEDURE

A. Required by Law refers to a mandate contained in law, and enforceable by a court, that compels Covered Entity to use or disclose PHI. This includes, but is not limited to, court orders, subpoenas issues by a court, grand jury, or administrative body authorized to require the production of information, and civil or investigative demands.

B. General Rule Regarding Use or Disclosure of PHI for Purposes Other Than Treatment, Payment or Health Care Operations. Under the Privacy Rule, Covered Entity may not disclose an Individual's PHI for purposes other than treatment, payment or health care operations without prior obtaining the Individual's prior written Authorization.

C. Exceptions to General Rule. In some situations, Covered Entity may have an obligation to disclose PHI pursuant to a federal, state or local law. PHI may be disclosed when required by one of these laws without obtaining the written Authorization of the Individual, and without providing the opportunity for the Individual to agree or object.

D. General Requirements for Use or Disclosure of PHI When Required By Law. Covered Entity may use or disclose PHI to the extent that such use or disclosure is Required by Law and the use or disclosure complies with and is limited to the relevant requirements of such law.

E. Examples of Disclosures Required By Law. Covered Entity may use or disclose PHI to the extent that such use or disclosure is required by law, including, but not limited to:

1) for public health activities Required by Law;

2) for disclosures about victims of abuse, neglect, or domestic violence;

3) in order to comply with a judicial or administrative request;

4) for health release;

5) to avert a serious threat to health or safety;

6) to comply with special government functions or requests.

F. Privacy Officer. When a Covered Entity employee believes that a use or disclosure of an Individual's PHI is Required by Law, the employee will confer with the Privacy Officer prior to making any such use or disclosure. The Privacy Officer will evaluate the proposed use or disclosure, in consultation with Covered Entity's legal counsel. No Covered Entity employee, regardless of title and/or position is authorized to use or disclose respond to such a request or to release information prior to forwarding the request on to the Privacy Officer.

G. Response to Request for Disclosure as Required By Law. Covered Entity personnel will refer or forward a request for disclosure of an Individual's PHI to the Privacy Officer after verifying the identity and authority of the requestor.

1) Prior to forwarding the request, the employee will verify the identity and authority of the Individual requesting PHI. No PHI shall be released in the absence of proper verification. See separate Policy and Procedure entitled "Verification of Identity". This information will be forwarded to the Privacy Officer along with the request for access.

2) If the identity and authority of the Individual requesting access to PHI cannot be verified, Covered Entity personnel will refer the issue to the Privacy Officer for immediate action.

3) Once the Privacy Officer has determined that use or disclosure of the PHI is appropriate, designated Covered Entity personnel with appropriate access clearance will be authorized to provide the requested PHI.

4) The requested PHI will be delivered to the requestor in a secure and confidential manner, such that information cannot be accessed by employees or other persons who do not have appropriate access clearance for the information provided.

H. The Privacy Officer will appropriately document the request for access and the delivery of the requested information**.**

RESEARCH USES AND DISCLOSURES POLICY

I. POLICY

Covered Entity shall comply at all times with the rules governing the Use or Disclosure of PHI for Research purposes. PHI may be Used or Disclosed for Research purposes only if either: (1) the Individual(s) who are the subject of the PHI provide Covered Entity with an appropriate Authorization for the Use or Disclosure; or (2) an Institutional Review Board or Privacy Board has approved a waiver of the need to obtain Authorization from the individual(s). Covered Entity personnel involved in Research must comply with this Policy at all times.

II. PURPOSE

The purpose of this Policy is to ensure that all Research conducted at Covered Entity facilities is performed in a manner that protects individual privacy and complies with all rules governing the Use or Disclosure of PHI in Research.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.512(i)

IV. PROCEDURE

A. Use of PHI for Research Purposes. Covered Entity personnel may not Use or Disclose PHI about an individual for Research purposes unless Covered Entity obtains either:

1) an Authorization from the individual covering the Research Uses and Disclosures. (For explanation about how to obtain an appropriate Authorization, please refer to Covered Entity Privacy Policy entitled Authorization or entitled Use and Disclosure of Protected Health Information); or

2) a waiver of the need for individual Authorization from an Institutional Review Board, in accordance with all of the requirements in Section B below.

In nearly all clinical trial research projects, in which the researcher has contact with the patient and the patient signs an informed consent, the researcher should obtain a separate Authorization for the Use or Disclosure of PHI regarding the subject. In other words, if Covered Entity can obtain Authorization to Use and Disclose PHI for Research Purposes, Covered Entity must obtain such Authorization. However, if it is not practicable to obtain Authorizations, the procedures described in Section B below are available.

B. Waiver of Authorization to Use and Disclose PHI for Research Purposes. Under some circumstances, Covered Entity may Use or Disclose PHI about an individual for Research without having an Authorization from that individual. Use or Disclosure of PHI for Research without an Authorization is permitted only if all of the following requirements of this Section B are met.

1) Waiver Approval by an Institutional Review Board. Any Use or Disclosure of PHI without an individual Authorization may be carried out only after a waiver of the need for Authorization has been approved by one of the following Boards:

a) An Institutional Review Board ("IRB") established in accordance with the federal Common Rule set forth at 45 C.F.R. Part 46; or

b) A Privacy Board that meets the following criteria:

i. the Board has members with varying backgrounds and appropriate professional competency to review the effect of the Research protocol on the privacy rights and interests of the Research subjects;

ii. the Board includes at least one member who is not affiliated with Covered Entity or any entity conducting or sponsoring the Research, and not related to any person who is affiliated with any of such entities; and

iii. the Board does not have any member participating in a review of any Research project in which the member has a conflict of interest.

In addition to approving a waiver of Authorization entirely, an IRB or Privacy Board may approve a waiver only in part or may approve only an alteration in the Authorization needed. In those circumstances, Covered Entity must obtain Authorizations to the extent needed to comply with the Board's partial waiver approval.

This IRB or Privacy Board review is in addition to any IRB approval that a Research protocol may need for purposes of human subject protection.

2) Documentation Requirements. To permit the Use or Disclosure of PHI pursuant to an IRB or Privacy Board waiver, Covered Entity must maintain the following documentation from the Board:

a) a written statement identifying the IRB or Privacy Board that approved the waiver and the date of the approval;

b) a written statement that the IRB or Privacy Board has determined that the waiver satisfies all of the following criteria:

i. the Use or Disclosure of PHI involves no more than minimal risk to privacy of the Research subjects, based on at least the presence of the following elements: (a) there is an adequate plan to protect Research subject identifying information from improper Use and Disclosure; (b) there is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the Research, unless there is a health or Research justification for retaining the identifiers or such retention is otherwise required by law; and (c) there are adequate written assurances that the PHI will not be reused or further Disclosed;

ii. the Research could not practicably be done without the waiver, i.e. it is not practicable to obtain Authorization; and

iii. the Research could not practicably be done without access to and Use of the PHI.

c) a brief description of the PHI that is necessary to be Used or Disclosed in order to practicably perform the Research;

d) a statement that the waiver has been approved under either normal or expedited procedures; and

e) the waiver must be signed by the chair of the IRB or Privacy Board, or another member of the IRB or Privacy Board as designated by the chair.

3) Normal and Expedited Review Procedures. An IRB or Privacy Board may approve a waiver under either: (1) normal review procedures; or (2) expedited review procedures, depending on the nature of the Research.

If the researcher uses an IRB established under the federal Common Rule, then the expedited and normal review procedures are governed by federal regulations at 45 C.F.R. §§46.108(b) and 46.110.

However, if a Privacy Board is used, then under normal procedures the Research must be reviewed at a meeting of the Privacy Board at which a majority of the Board members are present, including at least one member not affiliated with Covered Entity, not affiliated with any entity conducting or sponsoring the Research, and not related to any person who is affiliated with any of such entities. A majority of the members present at the meeting must approve the waiver.

Expedited procedures may be used only when the Research involves no more than minimal risk to the privacy of the Research subjects. If the Privacy Board elects to use expedited procedures, the waiver approval may be carried out by the Privacy Board chair, or by one or more members of the Privacy Board as designated by the chair.

All waiver approvals must include a statement indicated whether the approval was granted under normal or expedited review procedures.

C. Review Preparatory to Research. Researchers may have a need to review PHI in preparation for Research (such as for purposes of recruiting patients in a study), before a protocol or Research proposal is ready for submission to the IRB or Privacy Board. In these situations, Covered Entity may Use or Disclose PHI to a researcher without individual Authorization, so long as Covered Entity obtains from the researcher a written statement making the following representations:

1) the Use or Disclosure of PHI is sought solely to review Protected Health Information as necessary to prepare a Research protocol or for similar purposes preparatory to Research;

2) no PHI is to be removed from Covered Entity premises by the researcher in the course of the review; and

3) the PHI sought is necessary for the Research purposes.

D. Research Involving Deceased Individuals. Covered Entity may Use or Disclose PHI involving a deceased individual, so long as the researcher provides Covered Entity with the following:

1) a written representation that the Use or Disclosure of PHI is sought solely for Research involving the decedents;

2) documentation of the death of decedents; and

3) a written representation that the PHI sought is necessary for the Research purposes.

E. Illustrations:

Illustration #1: Physician A wishes to perform an archival medical records study to review patient outcomes over the past 15 years. Because there are no experimental or investigational procedures or items used, Physician A simply performs the research without obtaining either individual Authorization or IRB or Privacy Board review. Physician A performs the research and subsequently publishes an important article.

In this case, Physician A should have obtained either individual Authorizations or IRB or Privacy Board review. The study falls under the definition of Research because it is an investigation designed to contribute to generalizable knowledge, so Physician A may not Use Protected Health Information for that Research purpose without Authorization or Board approval: even if all of the Protected Health Information related to patients Physician A had treated.

Illustration #2: Physician A is participating as a principal investigator in an industry sponsored clinical trial. The research protocol involves an implant procedure and three follow up clinic visits. Each research subject signs an informed consent to participate in the research. Physician A has also arranged for each research subject to sign a separate Authorization to permit Physician A to Use and Disclose that individual's Protected Health Information for purposes of performing the protocol. Physician A obtains IRB approval of the research protocol to review human subject safety, but does not obtain IRB or Privacy Board waiver regarding subjects' privacy interests.

Physician A has complied with this Policy by obtaining individual Authorizations from each research subject to Use and Disclose Protected Health Information for Research purposes. IRB or Privacy Board waiver of Authorization is not needed if individual Authorizations are obtained. Moreover, an IRB or Privacy Board is unlikely to conclude that the Research could not practicably be done without a waiver, as required under this Policy, since Physician A has direct contact with each research subject and has plenty of opportunities to obtain individual Authorizations.

SPECIALIZED GOVERNMENT FUNCTIONS DISCLOSURES POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individuals' PHI. For most disclosures other than in the usual course of treatment, payment, or health care operations, Covered Entity must obtain the patient's Authorization before using or disclosing the patient's PHI. However, pursuant to certain specialized government functions, and subject to the requirements set forth in this Policy, PHI may be disclosed without the Authorization of the individual, or the opportunity for the individual to agree or object.

II. PURPOSE

The purpose of this policy is to provide guidance and ensure that any use or disclosure of PHI based on certain specialized government functions is in compliance with all applicable laws and regulations.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.512(k)
- National Security Act, 50 U.S.C. § 401, et seq.
- Executive Order 12333
- 18 U.S.C. § 3056
- 22 U.S.C. § 2709(a)(3)
- 18 U.S.C. § 871
- 18 U.S.C. § 879
- Executive Order 10450
- Executive Order 12968
- Foreign Service Act

IV. PROCEDURE

A. Public Benefits

1) Eligibility or Enrollment Information. Covered Entity may disclose PHI relating to eligibility for or enrollment in its health plan to another agency administering a government program providing health benefits if the sharing of eligibility or enrollment information among Covered Entity and the other agency or the maintenance of such information in a single combined data system accessible to all such government agencies is required or expressly authorized by a statute or regulation.

2) Same or Similar Populations. Covered Entity may disclose PHI relating to its health benefit program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

B. Other Specialized Government Functions

1) Military and Veterans Activities. Covered Entity may use and disclose PHI of individuals who are Armed Forces personnel or foreign military personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published the following information in the Federal Register: the appropriate military command authorities and the purposes for which the PHI may be used or disclosed.

2) National Security and Intelligence. Covered Entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).

3) Protective Services for the President and Others. Covered Entity may disclose PHI to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

4) Medical Suitability Determinations. Covered Entity may use PHI to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

   i. For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12968;
   ii. As necessary to determine worldwide availability or availability for mandatory service abroad under Sections 101(a) and 504 of the Foreign Service Act; or
   iii. For a family to accompany a Foreign Service member abroad, consistent with Sections 101(b)(5) and 904 of the Foreign Service Act.

5) Law Enforcement Custodial Situations.

   a) Disclosure to Correctional Institution. Covered Entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual PHI about that inmate or individual, if the correctional institution or law enforcement official represents that the PHI is necessary for:

      i. Provision of health care to such individuals;
      ii. The health and safety of such individual or other inmates;
      iii. The health and safety of the officers or employees of or others at the correctional institution;

iv. The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
v. Law enforcement on the premises of the correctional institution; or
vi. The administration and maintenance of the safety, security, and good order of the correctional institution.

b) Serving as a Correctional Institution. When Covered Entity serves as a correctional institution, it may use PHI of individuals who are inmates for any purpose for which such PHI may be disclosed.

c) Application after Release. For the purposes of this Section, Covered Entity will not consider an individual to be an inmate when released on parole, probation, supervised release, or when the individual is otherwise no longer in lawful custody.

SERIOUS THREAT TO HEALTH OR SAFETY DISCLOSURES POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individual's PHI. For most disclosures other than in the usual course of treatment, payment, or health care operations, Covered Entity must obtain the patient's Authorization before using or disclosing the patient's PHI. However, pursuant to serious threat to health or safety, and subject to the requirements set forth in this Policy, PHI may be disclosed without the Authorization of the individual, or the opportunity for the individual to agree or object.

II. PURPOSE

The purpose of this policy is to provide guidance and ensure that any use or disclosure of PHI based on a serious threat to health or safety is in compliance with all applicable laws and regulations.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.512(j)
- 45 C.F.R. § 164.501
- 45 C.F.R. § 164.512(f)(2)(i)

IV. PROCEDURE

A. General Rule Regarding Use or Disclosure of PHI Based on a Serious Threat to Health or Safety.

From time to time, Covered Entity may be requested to disclose PHI based on a serious threat to public health or safety.

Generally, Covered Entity may disclose PHI if Covered Entity, in good faith, believes the use or disclosure:

1) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

2) Is necessary for law enforcement authorities to identify or apprehend an individual:

   a) Because of a statement by an individual admitting participation in a violent crime that the Covered Entity believes may have caused serious harm to the victim; or
   b) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in 45 C.F.R. § 164.501.

B. Exceptions to General Rule.

Covered Entity may not disclose PHI in the event of a serious threat to health or safety if the information described in Section A of this policy is learned by the Covered Entity:

1) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling, or therapy; or

2) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy.

C. Limitation on Information Disclosed.

When disclosing information based on a serious threat to health or safety, Covered Entity shall only disclose the information described in Section A of this Policy and the following:

1) Name and address;

2) Date and place of birth;

3) Social Security Number;

4) ABO blood type and rh factor;

5) Type of injury;

6) Date and time of treatment;

7) Date and time of death, if applicable; and

8) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

D. Good Faith Requirement.

Covered Entity must only disclose information based on a serious threat to health or safety based on actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

BREACH NOTIFICATION POLICY

I. POLICY

Covered Entity recognizes that Individual rights are a critical component to maintaining quality care and service, and is committed to complying with the breach notification requirements of HIPAA. To support this commitment, Covered Entity maintains written Policies and Procedures to provide guidance to employees who are monitoring and reporting incidents of unauthorized Uses or Disclosures of Unsecured PHI.

II. PURPOSE

The purpose of this policy is to provide employees with guidance when monitoring and reporting incidents of unauthorized Use or Disclosure of Unsecured PHI.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.402 (Subpart D)

IV. PROCEDURE

A. Definition of a Breach and Unsecured PHI

Breach means the acquisition, access, Use, or Disclosure of unsecured PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI. Breach in all cases excludes:

1) Any unintentional acquisition, access, or Use of PHI by a workforce member or person acting under the authority of Covered Entity or a Business Associate, if such acquisition, access, or Use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under the Privacy Rule.

2) Any inadvertent Disclosure by a person who is authorized to access PHI at Covered Entity or Business Associate to another person authorized to access PHI at Covered Entity or Business Associate, or organized health care arrangement in which Covered Entity participates, and the PHI received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted under the Privacy Rule.

3) A Disclosure of PHI where Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such PHI.

Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in Department of Health and Human Services guidance, as updated from time to time (e.g., encryption, shredding).

B. Presumption of Breach and Risk Assessment Necessary to Demonstrate Low Probability of a Breach

If an acquisition, access, Use, or Disclosure of PHI in a manner not permitted by the Privacy Rule does not fall within any of the three exception set out in the definition of "Breach" above, then it is **presumed** to be a Breach unless Covered Entity or its Business Associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

2) The unauthorized person who Used the PHI or to whom the Disclosure was made.

3) Whether the PHI was actually acquired or viewed.

4) The extent to which the risk to the PHI has been mitigated.

C. Notification Procedures

1) Monitoring and Reporting Incidents of Unauthorized Acquisition, Access, Use or Disclosure of Unsecured PHI. Covered Entity will take reasonable steps to monitor the unauthorized acquisition, access, Use or Disclosure of Unsecured PHI. All workforce members shall be required to immediately report all suspected unauthorized acquisition, access, Uses or Disclosures to the Privacy Officer. Covered Entity will rely on its Business Associates to monitor and report incidents of unauthorized acquisition, access, Use or Disclosure of Unsecured PHI with respect to PHI the Business Associates acquires, accesses, Uses or Discloses, in accordance with the Breach Notification Requirements.

2) Determination Whether Unauthorized Acquisition, Access, Use or Disclosure Constitutes Breach. Upon receiving a report of unauthorized acquisition, access Use or Disclosure, the Privacy Officer, or his or her designee(s), will undertake a risk assessment to determine whether the unauthorized acquisition, access Use or Disclosure constitutes a Breach of Unsecured PHI. Covered Entity will make and retain records of such risk assessment and determinations, including the basis for determinations that unauthorized acquisition, access, Uses or Disclosures are not Breaches of Unsecured PHI. Covered Entity will rely on its Business Associates to determine whether incidents of unauthorized acquisition, access, Use or Disclosure of Unsecured PHI constitute a Breach with respect to PHI the Business Associate or one of its subcontractors acquires, accesses, Uses or Discloses, in accordance with the Breach Notification Requirements.

3) Notice to Affected Individuals of Breach. If the unauthorized acquisition, access, Use or Disclosure of Unsecured PHI is determined to constitute a Breach, the Privacy Officer, or his or her designee(s), will notify the Individual(s) whose Unsecured PHI was acquired, accessed, Used or Disclosed improperly in accordance with the Breach Notification Requirements via written notice, substitute notice or notice in urgent situations, as appropriate.

   a) Written Notice:

i. Written notices will be written in plain language and will include, to the extent possible:

1) a brief description of what happened, including the date of the Breach and the date of discovery of the Breach;
2) a description of the types of Unsecured PHI involved (without, however, including specific PHI);
3) any steps Individuals should take to prevent potential harm resulting from the Breach;
4) a brief description of what Covered Entity is doing (i) to investigate the Breach, (ii) to mitigate harm to Individuals and (iii) to protect against further Breaches; and
5) contact procedures for Individuals to ask questions or learn additional information, including a toll free telephone number, e-mail address, web site, or postal address.

b) Timing for Written Notice. Unless there is a law enforcement delay, such notification will be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach.

A Breach shall be treated as "discovered" by the Covered Entity as of the first day on which such breach is known to the Covered Entity, or, by exercising reasonable diligence would have been known to the Covered Entity. The Covered Entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or an agency of the Covered Entity.

c) Form of Notice. Notice required under this section to be provided to an Individual, with respect to a breach, shall be provided promptly and in the following form:

i. *First Class Notice.* Written notification by first-class mail to the Individual (or the next of kin of the Individual if the Individual is deceased) at the last known address of the Individual or the next of kin, respectively, or, if specified as a preference by the Individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

ii. *Notice In the Care of Insufficient or Out-of-Date Contact Information.* In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the Individual, electronic) notification to the Individual, a substitute form of notice shall be provided. In the case when there are 10 or more Individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period of ninety (90) days on the home page of the Web site of this Covered Entity or conspicuous notice in major print or broadcast media, including major media in geographic areas where

the Individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number that remains active for at least ninety (90) days, where an Individual can learn whether or not the Individual's unsecured PHI is possibly included in the breach.

iii. *Additional Notice in Urgent Situations*. In any case deemed by this Covered Entity to require urgency because of possible imminent misuse of unsecured PHI, this Covered Entity, in addition to notice provided under subparagraph (A), may provide information to Individuals by telephone or other means, as appropriate.

4) Notice to Media of Breaches Involving More Than 500 Residents of the Same State or Jurisdiction. If a Breach involves more than 500 residents of the same State or jurisdiction, the Privacy Officer, or his or her designee(s), will notify the media in accordance with the Breach Notification Requirements. Such notification will be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach.

5) Notice to Department of Health and Human Services of Breaches Involving 500 or More Individuals. If a Breach involves 500 or more Individuals, the Privacy Officer, or his or her designee(s), will notify the Department of Health and Human Services in the manner specified in the Breach Notification Requirements on the Department of Health and Human Services website. Such notification will be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach.

6) Maintenance of Log and Annual Notice to Department of Health and Human Services of Breaches Involving Less than 500 Individuals. The Privacy Officer, or his or her designee(s), shall maintain a log of Breaches involving less than 500 Individuals and, not later than 60 days after the end of each calendar year, shall notify the Department of Health and Human Services in the manner specified in the Breach Notification Requirements and on the Department of Health and Human Services website.

7) Breaches by Business Associates. Covered Entity may, as permitted by the Breach Notification Requirements, contract with Business Associates for Business Associates to undertake the notification requirements of this Policy and Procedure with respect to PHI acquired, accessed, Used or Disclosed by the Business Associate relating to Covered Entity, in addition to the obligations directly applicable to the Business Associates under the Breach Notification Requirements (including the obligations with respect to monitoring unauthorized Uses or Disclosures of PHI and making determinations whether such unauthorized Uses or Disclosures constitute a Breach.) If the Business Associate Agreement does not so provide, however, upon notification by a Business Associate of a Breach, the Privacy Officer, or his or her designee(s), shall undertake the notification requirements under this Policy to the extent necessary.

8) Law Enforcement Delay. If a law enforcement official determines that a notification, notice, or posting required under HIPAA would impede a criminal investigation or

cause damage to national security, such notification, notice, or posting shall be delayed as follows:

a) If law enforcement provides a written statement and specifies the time for which a delay is required, the Covered Entity or Business Associate shall delay such notification, notice or posting for the time period specified in writing.

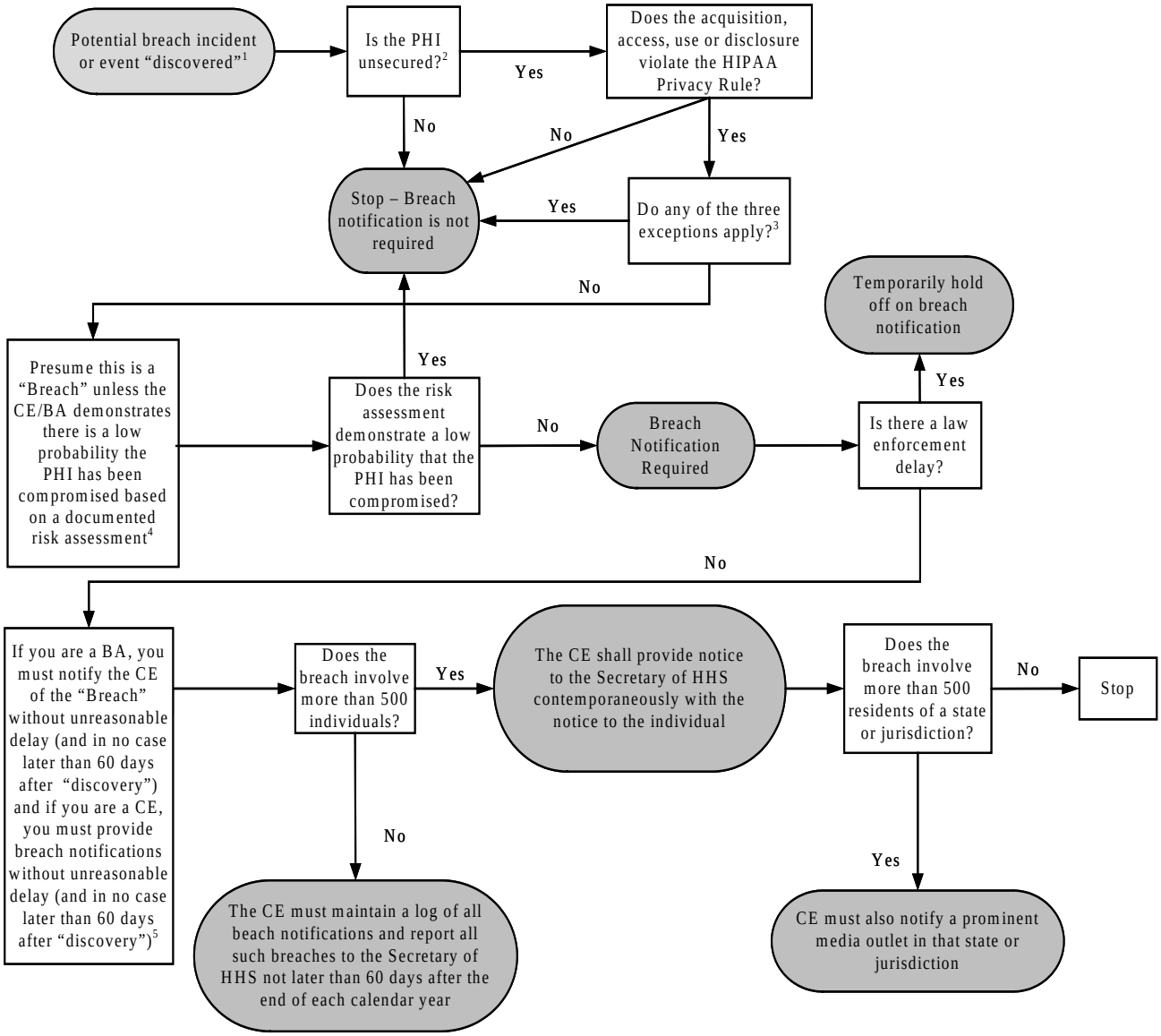
b) If the statement provided by law enforcement is only verbal, the Covered Entity or Business Associate must document the statement, and delay the notification, notice or posting temporarily and no longer than thirty (30) days from the date of the verbal statement, unless the law enforcement official provides a written statement.

INSTRUCTIONS FOR ANALYZING POTENTIAL BREACHES

1) Immediately, when a potential Breach is discovered, it shall be reported to the Privacy Officer.
2) The Privacy Officer will immediately investigate the matter to gain all possible facts related to the potential Breach in order to determine whether the potential Breach meets the definition of "Breach" under HIPAA. The attached Breach Notification Flowchart and Risk Assessment Tool can be used to assist in this process.
3) If it is determined that there was a Breach, notifications required under HIPAA as described in the Policy shall be made as soon as possible, and in no event greater than sixty days from the date of discovery.

SEE ATTACHED BREACH NOTIFICATION FLOWCHART, RISK ASSESSMENT TOOL, AND SAMPLE BREACH NOTIFICATION LETTER

BREACH NOTIFICATION FLOWCHART


Potential breach incident or event "discovered"[1]
Is the PHI unsecured?[2]
Yes
Does the acquisition, access, use or disclosure violate the HIPAA Privacy Rule?
No
No
Yes
Stop – Breach notification is not required
Yes
Do any of the three exceptions apply?[3]
No
Temporarily hold off on breach notification
Presume this is a "Breach" unless the CE/BA demonstrates there is a low probability the PHI has been compromised based on a documented risk assessment[4]
Yes
Does the risk assessment demonstrate a low probability that the PHI has been compromised?
No
Breach Notification Required
Is there a law enforcement delay?
Yes
No
If you are a BA, you must notify the CE of the "Breach" without unreasonable delay (and in no case later than 60 days after "discovery") and if you are a CE, you must provide breach notifications without unreasonable delay (and in no case later than 60 days after "discovery")[5]
Does the breach involve more than 500 individuals?
Yes
The CE shall provide notice to the Secretary of HHS contemporaneously with the notice to the individual
Does the breach involve more than 500 residents of a state or jurisdiction?
No
Stop
No
Yes
The CE must maintain a log of all beach notifications and report all such breaches to the Secretary of HHS not later than 60 days after the end of each calendar year
CE must also notify a prominent media outlet in that state or jurisdiction

[1.] A "Breach" is the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA's Privacy Rule which compromises the security or privacy of the PHI. 45 CFR 164.402

A Breach is "discovered" on the first day on which the breach is known by the CE/BA, or, by exercising reasonable diligence, would have been known. There is a 60-day clock from date of discovery to provide notification. 45 CFR 164.404(a)(2) & (b)

[2.] PHI is "unsecured" if it is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary. 45 CFR 164.402

[3.] The three exceptions are:

(i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or BA, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or OHCA in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in the manner not permitted under the Privacy Rule.

(iii) A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom disclosure was made would not reasonably have been able to retain such information. 45 CFR 164.402

[4.] The risk assessment must include at least an assessment of the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of a re-identification;

(ii) The unauthorized person who used the PHI or to whom the disclosure was made;

(iii) Whether the PHI was actually acquired or viewed; and

(iv) The extent to which the risk to the PHI has been mitigated. 45 CFR 164.402

[5.] Each Individual whose PHI has been, or is reasonably believed by the CE to have been, accessed, acquired, used, or disclosed must be notified:

(i) By 1st class mail (or electronic mail if the Individual has agreed to electronic notice). If the contact information is out-of-date or insufficient to provide written notice, the CE must provide a substitute notice that is reasonably calculated to reach the Individual (If the CE has insufficient contact information for less than 10 Individuals, the substitute notice may be by mail, phone or other means. If the CE has insufficient contact information for more than 10 Individuals, the substitute notice shall be either by a conspicuous posting on the CE website for at least 90 days, or in major print or broadcast media in the geographic areas where the Individuals likely reside).

(ii) If notice must be sent urgently because of possible imminent misuse of unsecured PHI, the CE may provide information by telephone or other means, as appropriate, in addition to written notice.

(iii) If the affected Individual is deceased, the CE must mail the notification by 1st class mail to the mailing address of the next of kin or personal representative (unless the contact information for the next of kin or personal representative is out-of-date or insufficient).

The Breach Notification must be written in plain language and must include the following information:

(i) A brief description of what happened (including the date of the Breach and date of discovery, if known);

(ii) A description of the types of unsecured PHI involved in the Breach;

(iii) Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

(iv) A brief description of the investigation, actions being taken to mitigate harm and protect against future breaches; and

(v) Contact procedure for more information.

BREACH RISK ASSESSMENT TOOL

Instructions:

This form must be completed thoroughly, in good faith, and the conclusion reached must be reasonable. For very simple incidents, this form may be completed by the Privacy Officer. If the incident is complicated, at least three Individuals (e.g., Privacy Officer and other members of the Compliance Committee) should independently complete this form, and meet to discuss their findings. Legal counsel should be consulted regarding breach risk assessments.

****

Date/Description of Incident:

_____

_____

_____

Factors to Consider:

1) What is the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification?
    a. HHS gave the following examples in the Final Rule: If you impermissibly disclosed a list of Individual names, addresses, and hospital identification numbers, the PHI is obviously identifiable, and a risk assessment would likely show more than a low probability the information was compromised. Alternatively, if you disclosed a list of Individual discharge dates and diagnoses, consider whether any of the Individuals could be identified based on the specificity of the diagnosis, the size of the community served, or whether the unauthorized recipient may have the ability to combine the information with other available information to re-identify the Individuals.

_____

_____

_____

_____

2) Who is the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made?
    a. HHS gave the following examples in the Final Rule: If you disclose PHI to another HIPAA-regulated entity, or a federal entity obligated to comply with the Privacy Act of 1974 or Federal Information Security Management Act of 2002, there may be a lower probability of compromise. However, if you disclose dates of health care service and diagnoses of certain employees with their employer, the employer may be able to determine that the information pertains to specific employees based on other information, such as dates of absence from work, creating a greater risk of compromise.

_____

_____

_____

_____

3) Have you investigated the impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed? Please explain.
    a. HHS gave the following examples in the Final Rule: If a laptop computer is stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, you can determine the PHI was not actually acquired, though the opportunity existed. However, if you mailed information to the wrong Individual who opened the envelope and called you to say she received the information in error, then she viewed and acquired the information because she opened and read it.

_____
_____
_____
_____

4) What is the extent to which the risk to the PHI has been mitigated?
    a. HHS gave the following examples in the Final Rule: If you misdirect a fax containing PHI to the wrong physician practice, and upon receipt, the receiving physician calls you to say he has received the fax in error and has destroyed it. HHS has said that though this scenario does not fit into any of the statutory or regulatory exception, HHS believes notification should not be required if you can demonstrate there is a low probability the data has been compromised. The extent of mitigation may depend on the assurances of those who received information in error. For example, you may be able to rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the entity or person destroyed the information it received in error, while such assurances from other third parties may not be sufficient.

_____
_____
_____
_____

5) Are there any other factors relevant to your analysis of this incident? Please list such factors below:

_____
_____
_____
_____

Based on consideration of the above factors, can we conclude there is a very low probability of compromise? (Please check yes or no).

☐ Yes: Explain why:

_____
_____

☐ No: Breach notification required.

****

Completed by: _____
Title: _____
Date: _____

SAMPLE BREACH NOTIFICATION LETTER

[LETTERHEAD]

VIA First Class Mail

[Date]

[Address]

Re: Breach Notification

Dear **[Individual/Next-of-Kin/Personal Representative]**:

[Provide brief description of what happened, including the date of the breach and the date it was discovered] This letter is to notify you that on _____ **[insert date of discovery]** we discovered that your PHI was improperly used or disclosed on or about _____ **[insert date of improper use/disclosure]**. Specifically, we discovered that [describe what happened].

[Provide a description of the types of unsecured PHI that were involved, such as full name, SSN, DOB, home address, account number, diagnosis, or other types of information] The following PHI was involved in the breach: _____.

[Provide a brief description of what you are doing to investigate the breach, to mitigate harm to the Individual, and to protect against further breaches. For example, who was notified and interviewed? What other steps are you taking to investigate the breach? Have you flagged the Individual's account or taken other measures to protect the Individual from further harm, such as offering free credit monitoring for the Individual for a period of time? Were applicable staff members or business associates notified/retrained? Were policies and procedures amended to reflect new safeguards related to preventing other similar breaches? etc.]

[Describe any steps the Individual should take to protect him or herself from potential harm resulting from the breach. For example, consider recommending that the Individual take steps to monitor the Individual's credit for a period of time.]

[Insert the contact procedures for Individuals to use if they have questions. This must include at least one of the following methods of contact: a toll-free telephone number, an email address, a web site, or a postal address.] If you have any questions or would like to talk to someone at _____ about this breach, please contact _____ at _____.

Sincerely,

BUSINESS ASSOCIATE ASSURANCES POLICY

I. POLICY

Covered Entity may disclose PHI to a Business Associate and may allow a Business Associate to create or receive PHI on its behalf. This Policy has been developed to ensure the privacy and security of PHI when Covered Entity is disclosing PHI to its Business Associates.

II. PURPOSE

The purpose of this Policy is to provide guidance to employees on the requirements of HIPAA as it relates to the Disclosure of PHI to Business Associates to ensure compliance with HIPAA.

III. REFERENCES /CROSS-REFERENCES

- 45 C.F.R. §164.502(e)
- 45 C.F.R. §164.504(e)
- 45 C.F.R. §164.308(b)
- 45 C.F.R. §164.314(a)

IV. PROCEDURES

A. Definition of Business Associate

Business Associate means any entity or person who, on behalf of Covered Entity (but other than in the capacity of a member of the Covered Entity's workforce), creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, Individual safety activities, billing, benefit management, practice management, and repricing, or uses PHI to provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Covered Entity. It includes a health information organization, e-prescribing gateway or other entity or person who provides data transmission services with respect to PHI and that requires access on a routine basis to such PHI. It does not, however, include an officer, director, or employee of Covered Entity. It includes a person that offers a personal health record on behalf of the Covered Entity. It includes a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

B. Business Associate Contracts.

Covered Entity shall ensure contracts or other arrangements between Covered Entity and its Business Associates comply with the Policies and Procedures described herein and pursuant to the HIPAA. Specifically:

1) Covered Entity shall document satisfactory assurances of compliance with the Policies and Procedures herein through a written contract or other written agreement or arrangement with the Business Associate that establishes permitted and required Uses and Disclosures of PHI.

2) Written contracts or agreements between Covered Entity and a Business Associate shall provide that the Business Associate shall:

a) not Use or further Disclose PHI other than as permitted or required by the contract or as required by law;
b) use appropriate safeguards and comply with Security Rule with respect to PHI in electronic form to prevent Use or Disclosure of PHI other than as provided for by its contract;
c) report to the Covered Entity any Use or Disclosure of PHI not provided for by its contract of which it becomes aware, including security incidents and breaches of unsecured PHI as required by 45 C.F.R. § 164.410;
d) ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions and conditions that apply to the Business Associate with respect to such PHI by entering into a contract or other arrangement that complies with HIPAA;
e) make available PHI in accordance with the Individual's right to access such information, including to incorporate any amendments to PHI and to provide an accounting of disclosures in accordance with the Individual's right to request an amendment to PHI or an accounting of disclosures;
f) to the extent the Business Associate is to carry out the Covered Entity's duties under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such duties;
g) make its internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received by the Business Associate on behalf of the Covered Entity available to the Department of Health and Human Services for purposes of determining Covered Entity's compliance with the Privacy Rule;
h) at termination of the contract, if feasible, return or destroy all PHI received from, created, or received by the Business Associate on behalf of Covered Entity that the business associate maintains in any form and retain no copies of such information, or if such return or destruction is not feasible, extend the protections of the contract to the PHI and limit further Uses and Disclosures to those purposes that make the return or destruction of the PHI infeasible.
i) authorize termination of the contract by Covered Entity if Covered Entity determines that the Business Associate has violated a material term of the contract.

3) Use of PHI by Business Associate. At the sole discretion of Covered Entity, contracts or agreements between Covered Entity and a Business Associate may permit the Business Associate to do the following:

a) provide data aggregation services relating to the health care operations of Covered Entity;
b) Use the PHI received in its capacity as a Business Associate to Covered Entity, if necessary for the proper management and administration of the

Business Associate or to carry out the legal responsibilities of the Business Associate;

c) Disclose PHI if necessary for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate if the Business Associate obtains reasonable assurances from the person to whom the PHI is Disclosed that it will be held confidentially and Used or further Disclosed only as required by law or for the purpose for which it was Disclosed. The person to whom the PHI is Disclosed must notify the Business Associates of any instances of which it is aware that the confidentiality of the information has been breached; and

d) Disclose PHI if law requires the Disclosure.

4) Obligation To Cure Breach. Covered Entity, upon learning that a pattern of activity or practice of a Business Associate constitutes a material breach or violation of the Business Associate's obligation under the contract or other arrangement, will take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful, terminate the contract or arrangement, if feasible.

5) Entering into Business Associate Agreements. No employee is authorized to enter into a contract with a Business Associate without the prior approval of the contract from the Privacy Officer or Covered Entity's legal counsel. Any employee who is in receipt of such a contract from a Business Associate will forward the same to the Privacy Officer immediately.

6) When Both Entities are Governmental Entities. If the Covered Entity and Business Associate are both governmental entities, the Covered Entity may enter into a memorandum of understanding with the business associate that contains the same terms and objectives as set out in this Policy.

INSTRUCTIONS

1. Before disclosing any PHI to a third party who is providing services on behalf of the Covered Entity, or assisting the Covered Entity is performing services, members of the workforce should contact the Privacy Officer to determine whether the third party is a business associate.

2. If it is determined that the third party is a business associate, the Privacy Officer will provide the third party with the attached business associate agreement. The third party must sign the business associate agreement prior to having any access to PHI.

3. If the third party desires to revise or amend the business associate agreement, the Privacy Officer should be contacted to evaluate whether any amendments will be permitted.

SEE ATTACHED BUSINESS ASSOCIATE AGREEMENT TEMPLATE

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is entered into by and between Central Iowa Community Services (the "Covered Entity"), and _____ (the "Business Associate").

RECITALS

A. Covered Entity is a health care provider subject to the Health Insurance Portability and Accountability Act of 1996, the HITECH Act, and regulations promulgated thereunder ("HIPAA").

B. Business Associate, through the provision of certain services for or on behalf of the Covered Entity pursuant to a certain agreement entered into with Covered Entity on _____ for the provision by Business Associate of _____ services for Covered Entity (the "Services Agreement"), is a "business associate" of the Covered Entity as that term is defined in 45 C.F.R. § 160.103, and is subject to the Security Rule and certain provisions of the Privacy Rule.

C. Covered Entity is required by HIPAA to obtain satisfactory assurances that Business Associate will appropriately safeguard all PHI and Electronic PHI disclosed by, or created or received by Business Associate on behalf of, Covered Entity.

NOW, THEREFORE, in consideration of entering into the Services Agreement and the mutual promises and agreements below and in order to comply with all legal requirements, the parties agree as follows:

I. DEFINITIONS

1.1 "Agreement" has the meaning set forth in the preamble.

1.2 "**ARRA Breach**" has the same meaning as the term "Breach" in Section 13400(1) of the HITECH Act (i.e. 42 USCA 17921) and 45 CFR 164.402.

1.3 "**Business Associate**" has the meaning set forth in the preamble.

1.4 "**Covered Entity**" has the meaning set forth in the preamble.

1.5 "**Data Aggregation**" means the combining of PHI created or received under this Agreement with the PHI Business Associate receives or creates in its arrangement with another covered entity under the Privacy Rule to permit data analysis that relate to the Health Care Operations of the covered entities.

1.6 "**Designated Record Set**" means a group of records maintained by or for the Covered Entity that is: (i) the medical records and billing records about Individuals; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. As used herein the term "record" means any item, collection,

or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the Covered Entity.

1.7 "**Document Demand**" has the meaning set forth in Section 3.13.

1.8 "**Effective Date**" has the meaning set forth in the preamble.

1.9 "**Electronic PHI**" means information that comes within paragraphs 1(i) or 1(ii) of the definition of "PHI," as defined in 45 C.F.R. § 160.103, limited to the information created, received, maintained or transmitted by Business Associate on behalf of Covered Entity.

1.10 "**HIPAA**" has the meaning set forth in the Recitals.

1.11 "**HITECH Act**" means Title XIII and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law No. 111-5 and all regulations promulgated thereunder.

1.12 "**Individual**" means the person who is the subject of the PHI and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.13 "**PHI**" means Protected Health Information that is provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity.

1.14 "**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.

1.15 "**Protected Health Information**" (or "PHI") means any information, whether transmitted or maintained in electronic, written, oral, or any other form or medium, that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual; and (i) identifies the Individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

1.16 "**Required by Law**" has the same meaning as the term "'required by law" in 45 C.F.R. § 164.103.

1.17 "**Secretary**" means the Secretary of the U.S. Department of Health and Human Services or his or her designee.

1.18 "**Security Incident**" has the same meaning as the term "security incident" in 45 C.F.R. § 164.304.

1.19 "**Security Rule**" means the Security Standards and Implementation Specifications at 45 C.F.R. part 160 and part 164, subpart C.

1.20 "**Services Agreement**" has the meaning set forth in the Recitals.

1.21 "**Unsecured PHI**" or "**Unsecured PHI**" means PHI that is not secured through the use of a technology or methodology that the Secretary specifies in guidance renders PHI unusable,

unreadable, or indecipherable to unauthorized Individuals, such as the guidance set forth in 74 Fed. Reg. 19006 (April 27, 2009) and updated in 74 Fed. Reg. 42740 (August 24, 2009).

1.22 Remaining Terms. Capitalized terms used, but not otherwise defined, in this Agreement have the meaning ascribed to them in HIPAA, the Privacy Rule, the Security Rule or the HITECH Act.

II. PERMITTED USES AND DISCLOSURES OF PHI

2.1 Services Agreement Uses and Disclosures. Business Associate may use or disclose PHI for purposes of performing its obligations and functions under the Services Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

2.2 Other Permitted Uses. If necessary, Business Associate may use PHI: (i) for the proper management and administration of the Business Associate; (ii) to carry out the legal responsibilities of the Business Associate; and (iii) for the provision of Data Aggregation services relating to the Health Care Operations of Covered Entity.

2.3 Other Permitted Disclosures. If necessary, Business Associate may disclose PHI for the purposes described in Section 2.2 above if: (i) the disclosure is Required by Law; or (ii) Business Associate obtains reasonable written assurance from the person or entity to whom it discloses the PHI that the PHI will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person or entity, and the person or entity notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

III. OBLIGATIONS OF BUSINESS ASSOCIATE

3.1 Compliance with Privacy Rule. Business Associate shall comply with all applicable provisions of the Privacy Rule in carrying out its obligations under the Services Agreement and this Agreement. Further, to the extent Business Associate is to carry out any of Covered Entity's obligations under subpart E of 45 CFR 164, Business Associate agrees to comply with the requirements of such subpart that apply to Covered Entity in the performance of such obligations.

3.2 Prohibition on Unauthorized Use or Disclosure. Business Associate shall not use or disclose PHI except as permitted by this Agreement or as Required by Law.

3.3 Minimum Necessary.

3.3.1 Business Associate shall limit its use and disclosure of PHI under this Agreement to the "minimum necessary," as set forth in guidance that the Secretary will issue regarding what constitutes "minimum necessary" under the Privacy Rule. Until the issuance of such guidance, Business Associate shall limit its use and disclosure of PHI, to the extent practicable, to the Limited Data Set (as that term is defined in 45 C.F.R. § 164.514(e)(2)), or, if needed, to the minimum necessary to accomplish the Business Associate's intended purpose. Business Associate may in good faith determine what

constitutes the minimum necessary to accomplish the intended purpose of any disclosure of PHI.

3.3.2 Paragraph (a) above does not apply to: (1) disclosures to or requests by a health care provider for treatment; (2) uses or disclosures made to the Individual; (3) disclosures made pursuant to an authorization as set forth in 45 C.F.R. § 164.508; (4) disclosures made to the Secretary under 45 C.F.R. part 160, subpart C; (5) uses or disclosures that are Required by Law as described in 45 C.F.R. § 164.512(a); and (6) uses or disclosures that are required for compliance with applicable requirements of the Privacy Rule.

3.4 Safeguarding PHI; Security Regulations. Business Associate shall use appropriate administrative, physical, and technical safeguards and comply with the Security Rule with respect to Electronic PHI to prevent the use or disclosure of PHI other than as provided for by this Agreement.

3.5 Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Security Incident or a use or disclosure of PHI by Business Associate in violation of this Agreement.

3.6 Reporting. In the event that Business Associate becomes aware of a use or disclosure of PHI by Business Associate that is not permitted under this Agreement, Business Associate shall report such use or disclosure to the Covered Entity promptly in writing and in any event, within 5 days of becoming aware of the use or disclosure. Business Associate agrees to report to Covered Entity in writing any Security Incident of which it becomes aware, except that, for purposes of this reporting requirement the term "Security Incident" does not include inconsequential incidents that occur on a frequent basis such as scans or "pings" that are not allowed past Business Associate's firewall. Notwithstanding this Section 3.7, the Business Associate's reporting obligations regarding any ARRA Breach are set forth in Article IV.

3.7 Subcontractors. Business Associate shall ensure that all subcontractors or agents of Business Associate that create, receive, maintain or transmit PHI on behalf of the Business Associate agree in writing to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Business Associate shall ensure that all agents, including subcontractors, to whom it provides Electronic PHI, agree in writing to implement reasonable and appropriate safeguards to protect such Electronic PHI.

3.8 Access.

3.8.1 Within twenty (20) days of a request from Covered Entity, Business Associate shall furnish the PHI contained in a Designated Record Set that will enable the Covered Entity to respond to an Individual's request for inspection or copies of PHI about the Individual pursuant to 45 CFR § 164.524.

3.8.2 In the event an Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to the Covered Entity immediately and take no direct immediate action on any such request. If the Covered Entity determines that an Individual is to be granted access to PHI, then Business Associate shall

cooperate with the Covered Entity to provide to any Individual, at the Covered Entity's direction, any PHI requested by such Individual.

3.9 Amendment.

3.9.1 If the Covered Entity requests that Business Associate amend any Individual's PHI or a record regarding an Individual contained in a Designated Record Set, then Business Associate shall provide the relevant PHI to the Covered Entity for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526.

3.9.2 In the event an Individual requests directly to Business Associate that PHI be amended, Business Associate shall forward such request to the Covered Entity within ten (10) days of Business Associate's receipt of such request and shall take no direct immediate action on the request.

3.10 Records Availability. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining compliance with the Privacy Rule and the Security Rule.

3.11 Accounting of Disclosures.

3.11.1 If the Covered Entity requests that Business Associate furnish an accounting of disclosures of PHI made by Business Associate regarding an Individual during the six (6) years prior to the date on which the accounting was requested, then Business Associate shall, within fifteen (15) days of such request, make available to the Covered Entity such information as is in Business Associate's possession and is required for the Covered Entity to make the accounting required by 45 C.F.R. §164.528 and future regulations to be promulgated regarding accounting of disclosures.

3.11.2 In the event an Individual requests an accounting of disclosures directly from Business Associate, Business Associate shall within ten (10) days forward such request to the Covered Entity and shall take no direct action on the request.

3.12 Demands for Production of PHI.

3.12.1 Receipt by Business Associate. If Business Associate receives a subpoena, civil or administrative demand, or any other demand for production of PHI (a "Document Demand"), Business Associate shall provide a copy of such Document Demand to Covered Entity within five (5) days of receipt. To the extent the PHI that is the subject of the Document Demand is in the possession of Business Associate, and a response is warranted according to the standards contained in 45 C.F.R. § 164.512(e), Business Associate shall timely respond to the Document Demand.

3.12.2 Receipt by Covered Entity. If Covered Entity receives a Document Demand, Business Associate shall provide to Covered Entity any PHI responsive to such Document Demand and assist and cooperate with Covered Entity in responding to such

Document Demand in a timely manner and in accordance with the standards under 45 C.F.R. § 164.512(e).

3.13 Request for Restrictions on Disclosure of PHI. As required by Section 13405 of the HITECH Act and 45 CFR 164.522 (except as otherwise required by law), Business Associate shall comply with any request of an Individual for the Business Associate to restrict the disclosure of PHI of the Individual when the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment), and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

3.14 Remuneration for PHI.

3.14.1 Except as explicitly permitted in the Services Agreement and also set forth in paragraph (b) below, Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI of an Individual unless the Individual provided to the Covered Entity a valid authorization in accordance with 45 C.F.R. § 164.508 that specifically authorizes the Business Associate to exchange the PHI for remuneration.

3.14.2 Paragraph (a) above does not apply if the purpose of the exchange is: (1) for public health purposes pursuant to 45 CFR § 164.512(b) or § 164.514(e); (2) for research purposes pursuant to 45 CFR § 164.512(i) or § 164.514(e), where the only remuneration received by the Covered Entity or Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes; (3) for treatment and payment purposes pursuant to 45 CFR § 164.506(a); (4) for the sale, transfer, merger, or consolidation of all or part of the Covered Entity and for related due diligence as described in the HIPAA definition of health care operations and pursuant to 45 CFR § 164.506(a); (5) To or by a Business Associate for activities that the Business Associate undertakes on behalf of a Covered Entity (or on behalf of a Business Associate in the case of a subcontractor), pursuant to 45 CFR §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the Covered Entity to the Business Associate (or by the Business Associate to the subcontractor, if applicable), for the performance of such activities; (6) to an Individual, when the Individual requests access to his or her PHI pursuant to 45 CFR § 164.524 or when the Individual requests an accounting of disclosures pursuant to 45 CFR § 164.528; (7) for disclosures Required By Law; and (8) for any other purpose permitted by HIPAA where the only remuneration received by the Covered Entity or Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee expressly permitted by law.

3.15 Marketing Restrictions. Business associate shall ensure that any Marketing communications it makes on behalf of Covered Entity are in compliance with the rules governing marketing set forth in 45 C.F.R. 164.508(a)(3), including but not limited to the requirements that Business Associate must obtain an authorization from an Individual prior to making any marketing communication to such Individual.

3.16 Fundraising Limitations. Business Associate shall ensure that any fundraising communications Business Associate makes on behalf of the Covered Entity are in compliance with the rules governing fundraising communications set forth in 45 C.F.R. 164.514(f), including but

not limited to the requirement that Business Associate must provide, with each fundraising communication made to an Individual, a clear and conspicuous opportunity for the recipient of the communication to elect not to receive any further fundraising communications. Business Associate shall ensure that all Individuals electing not to receive any further fundraising communications do not receive any further fundraising communications.

IV. ARRA BREACH NOTIFICATION.

4.1 Risk Assessment by Business Associate. If Business Associate becomes aware of a potential ARRA Breach, Business Associate shall complete a risk assessment of the potential ARRA Breach to determine whether the potential ARRA Breach is an ARRA Breach. Such risk assessment shall include at least all the factors identified in 45 CFR 164.402(2), as amended by the final rule published in the Federal Register on January 25, 2013 at 78 Fed. Reg. 5566.

4.2 Notification to Covered Entity. If, after completing such risk assessment, Business Associate concludes that there was an ARRA Breach, Business Associate shall notify the Covered Entity of the ARRA Breach as soon as reasonably possible, and in all cases within five (5) business days of the first day on which any employee, officer or agent of Business Associate either knows or by exercising reasonable diligence would have known that an ARRA Breach occurred. The notification to Covered Entity shall include, if known, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed during such ARRA Breach. The notification shall also include: (a) a brief description of what happened, including the date of the ARRA Breach and the date of the discovery of the ARRA Breach, if known; (b) a description of the types of Unsecured PHI that were involved in the ARRA Breach (such as whether the full name, social security number, date of birth, home address, account number, diagnosis disability code or other types of information were involved); (c) recommended steps that Individuals should take to protect themselves from potential harm resulting from the ARRA Breach; and (d) a brief description of what the Business Associate is doing to investigate the ARRA Breach, to mitigate harm to Individuals, and to protect against any further ARRA Breaches. Business Associate shall maintain evidence to demonstrate that any required risk assessment was completed and notification to the Covered Entity under this paragraph was made unless the Business Associate determines that a delayed notice (as described in Section 4.3) applies.

4.3 Delayed Notification to Covered Entity. Notwithstanding Section 4.2 above, if a law enforcement official states in writing to Business Associate that the notification to Covered Entity required under Section 4.2 would impede a criminal investigation or cause damage to national security, then Business Associate may delay the notification for any period of time set forth in the written statement of the law enforcement official. If the law enforcement official provides an oral statement, then Business Associate shall document the statement in writing, including the name of the law enforcement official making the statement, and may delay the notification required under Section 4.2 for no longer than thirty (30) days from the date of the oral statement, unless the law enforcement official provides a written statement during that time that specifies a different time period. Business Associate shall be obligated to maintain evidence to demonstrate the reason for the delayed notification and that the required notification under this paragraph was made

4.4 Notification to Individuals, the Secretary and/or the Media. In the event of an ARRA Breach caused by Business Associate, its agents and/or subcontractors, Business Associate shall provide assistance to Covered Entity in making all ARRA Breach notifications. To the extent Covered Entity incurs expenses and costs to comply with its notification obligations with respect to an ARRA Breach by Business Associate, its agents and/or subcontractors, in addition to any other remedies that may be available to Covered Entity under this Agreement or any applicable law, Business Associate shall reimburse Covered Entity for all costs and expenses (including attorneys' fees) incurred by Covered Entity related to providing the notifications required under 45 C.F.R. §§ 164.404, 406 and 408. Notwithstanding the foregoing, if the parties agree that Business Associate will, on behalf of Covered Entity, and within the applicable time frames required by law under 45 C.F.R. §§ 164.404, 406 and 408, prepare and send out any and all required ARRA Breach notifications to Individuals, the Secretary and/or to the media, Business Associate shall prepare and send such ARRA Breach notifications at Business Associate's sole expense and in compliance with the requirements of 45 C.F.R. 164.404, 406 and 408, as applicable. However, any ARRA Breach notifications Business Associate would prepare and send on behalf of Covered Entity shall be subject to Covered Entity's review and pre-approval before the notifications are sent. Additionally, in the event of an ARRA Breach, Business Associate agrees to pay for the credit monitoring fees for affected Individuals for a period of at least two (2) years of credit monitoring.

V. TERM AND TERMINATION

5.1 Term. This Agreement is effective upon the effective date of the Services Agreement, and except for the rights and obligations set forth in this Agreement specifically surviving termination, shall terminate the later of the date the Services Agreement terminates or when all PHI is returned to Covered Entity or, with prior permission of Covered Entity, destroyed.

5.2 Termination for Cause. Notwithstanding any provision in this Agreement, Covered Entity may terminate this Agreement and the Services Agreement if Covered Entity determines, in its sole discretion, Business Associate has breached any provision of this Agreement or otherwise violated HIPAA, the Privacy Rule, the Security Rule or the HITECH Act. Covered Entity shall provide written notice to Business Associate with an opportunity for Business Associate to cure the breach or end the violation within ten (10) business days of such written notice, unless cure is not possible. If Business Associate fails to cure the breach or end the violation within the specified time period, or if cure is not possible, this Agreement and the Service Agreement shall automatically and immediately terminate, unless termination is infeasible.

5.3 Termination after Repeated Violations. Notwithstanding any provision in the Agreement, Covered Entity may terminate the Services Agreement and this Agreement if Covered Entity determines, in its sole discretion, that Business Associate has repeatedly breached any provision of this Agreement or otherwise violated HIPAA, the Privacy Rule, the Security Rule or the HITECH Act, irrespective of whether, or how promptly, Business Associate may remedy such violation after being notified of the same.

5.4 Obligations Upon Termination. Business Associate's obligations to protect the privacy and security of PHI shall be continuous and shall survive termination, cancellation, expiration or other conclusion of this Agreement or the Services Agreement. Upon termination of this Agreement, Business Associate will forward to Covered Entity, or to Covered Entity's

designee, the records necessary for continued administration of Covered Entity as directed by Covered Entity. After the forwarding of said records, whatever PHI remains with Business Associate will be subject to the following:

5.4.1 Except as provided in paragraph (b) of this Section 5.4, upon termination, cancellation, expiration or other conclusion of this Agreement, for any reason, Business Associate shall return or, if Covered Entity gives written permission, destroy, PHI in whatever form or medium and retain no copies of such PHI. Business Associate will complete such return or destruction as soon as possible, but in no event later than sixty (60) days from the date of the termination of this Agreement. Within ten (10) days of the return or destruction of all PHI by Business Associate, Business Associate shall provide written certification to Covered Entity that the return or destruction of PHI has been completed.

5.4.2 In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VI. INDEMNIFICATION; INSURANCE

6.1 Indemnification by Business Associate. Business Associate will indemnify and hold harmless Covered Entity, and any affiliate, officer, director, employee or agent of Covered Entity from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any use or disclosure of PHI that violates or is not permitted by this Agreement, HIPAA, the Privacy Rule, the Security Rule or the HITECH Act, or other breach of this Agreement by Business Associate or any subcontractor or agent of Business Associate.

6.2 Right to Tender or Undertake Defense. If Covered Entity is named as a party in any judicial, administrative or other proceeding arising out of or in connection with any non-permitted or violating use or disclosure of PHI or other breach of this Agreement by Business Associate or any subcontractor or agent of Business Associate, Covered Entity shall have the option at any time either to: (i) tender its defense to Business Associate, in which case Business Associate will provide qualified attorneys, consultants, and other appropriate professionals to represent Covered Entity's interests at Business Associate's expense; or (ii) undertake its own defense, choosing the attorneys, consultants, and other appropriate professionals to represent its interests, in which case Business Associate will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants, and other professionals.

6.3 Right to Control Resolution. Covered Entity has the sole right and discretion to settle, compromise or otherwise resolve any and all claims, causes of actions, liabilities or damages against it, notwithstanding that Covered Entity may have tendered its defense to Business Associate. Any such resolution will not relieve Business Associate of its obligation to indemnify Covered Entity under this Agreement.

6.4 Insurance. Upon request, Business Associate shall obtain and maintain insurance coverage against improper uses and disclosures of PHI by Business Associate, naming Covered Entity as an additional named insured. Upon request, Business Associate shall provide a certificate evidencing such insurance coverage.

6.5 Conflicts. With respect to any breaches or violations of this Agreement, the provisions in this Section 6 supersede any inconsistent terms contained in the Services Agreement.

VII. GENERAL PROVISIONS

7.1 Effect. The terms and provisions of this Agreement supersede any other conflicting or inconsistent terms and provisions in any agreements between the parties, including all exhibits or other attachments thereto and all documents incorporated therein by reference.

7.2 Amendment. Business Associate and the Covered Entity agree to amend this Agreement to the extent necessary to allow either party to comply with HIPAA, the Privacy Rule, the Security Rule, or the HITECH Act. All such amendments shall be made in a writing signed by both parties.

7.3 No Third Party Beneficiaries. This Agreement is intended for the benefit of Business Associate and Covered Entity only. Nothing express or implied is intended to confer or create, nor be interpreted to confer or create, any rights, remedies, obligations or liabilities to or for any third party beneficiary, including without limitation Individuals who are the subject of PHI.

7.4 Severability. In the event that any provision of this Agreement violates any applicable statute, ordinance, or rule of law in any jurisdiction that governs this Agreement, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this Agreement.

7.5 No Waiver. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.

7.6 Assignment. This Agreement may not be assigned by either party without the prior written consent of the other party; provided, however, that the parties shall cooperate to assign this Agreement as appropriate if the Services Agreement is assigned.

7.7 Relationship of the Parties. Business Associate and Covered Entity are independent contractors and all acts performed by Business Associate are performed solely in its capacity as an independent contractor.

7.8 Counterparts; Facsimile Signature. This Agreement may be executed by facsimile and/or in counterparts, each of which shall be an original and all of which together shall constitute one and the same binding instrument.

7.9 Notification

7.9.1 Business Associate. To the extent notice is required to be provided by Covered Entity to Business Associate under any provision in this Agreement, notice shall be provided to:

_____
_____
_____
_____

7.9.2 Covered Entity. To the extent notice is required to be provided by Business Associate to Covered Entity under any provision in this Agreement, notice shall be provided to:

Russell Wood
russell.wood@cicsmhds.org
123 1st Ave SW, (PO Box58)
Hampton IA 50441
641-456-2128
Fax 641-456-2852

7.10 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA, the Privacy Rule, the Security Rule, and the HITECH Act.

INTENDING TO BE LEGALLY BOUND, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

BUSINESS ASSOCIATE

_____

By: _____

Print Name: _____

Title: _____

Date: _____

COVERED ENTITY

[NAME]

By: _____

Print Name: _____

Title: _____

Date: _____

COMPLAINTS, NON-RETALIATION AND WAIVER OF RIGHTS POLICY

I. Policy

Covered Entity recognizes that Individual rights are a critical component to maintaining quality care and service, and is committed to allowing Individuals to exercise their rights under applicable federal, state and/or local laws and regulations. To support this commitment, Covered Entity maintains written Policies and Procedures to provide guidance to Covered Entity's employees when faced with a complaint by an Individual regarding Covered Entity's use or disclosures of the Individual's PHI.

II. PURPOSE

HIPAA requires the Covered Entity to have a mechanism for receiving complaints from Individuals regarding Covered Entity's compliance with the Privacy Rule. We are required to accept complaints about any aspect of our practices regarding PHI. The purpose of this Policy is to provide guidance to employees when faced with an Individual wishing to make a complaint. Another purpose of this Policy is to ensure that no employee engages in intimidating, threatening coercive or discriminatory against any Individual for exercising their rights under HIPAA, including the filing of a complaint. A further purpose of this policy is to inform employees that Individuals cannot be required to waive their rights under HIPAA as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §530(d)

IV. PROCEDURE

A. Individual's Right to File a Complaint. Under the Privacy Rule, the Individual has a right to file a complaint with Covered Entity regarding Covered Entity's use or disclosure of the Individual's PHI.

1) **Form of Complaint**. An Individual desiring to file a complaint should be provided with Covered Entity's Complaint Form.

2) **Verbal Complaint**. If an Individual refuses to complete the Complaint form, but wishes to make a complaint, the employee shall give the Individual the name, or title, and telephone number of the Privacy Officer, or designee.

3) **No Waiver**. Covered Entity shall not require Individuals to waive their right to file a complaint with the Department of Health and Human Services as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

B. Report of Concern by Workforce Members and Agents of Covered Entity. The Covered Entity believes that an effective system of communication is important in identifying compliance violations of the privacy standards adopted by the Covered Entity to protect PHI. To encourage communication of compliance concerns by members of the

workforce and other agents doing business with the Covered Entity, the Covered Entity has implemented a reporting system that permits the workforce and other agents to report concerns openly or anonymously, verbally or in writing, in accordance with established procedures.

The Covered Entity will make every reasonable effort to protect the identity of a reporting employee, unless the employee permits the Covered Entity to reveal their identity. However, no guarantee of anonymity can be assured. No disciplinary action or retaliation will be taken against an employee who makes a good faith report of a compliance concern.

A report of concern may be made by anyone having knowledge or information about a known or suspected violation of the Covered Entity's privacy standards or the laws and regulations governing the Covered Entity. Reports may be made verbally or in writing to the Covered Entity privacy officer or to Office for Civil Rights, U.S. Department of Health and Human Services, 601 East 12th Street--Room 248, Kansas City, Missouri 64106. Voice Phone (816) 426-7278. FAX (816) 426-3686. TDD (816) 426-7065. All reports, whether verbal or written, will be documented on the Confidential Report of Concern, attached hereto.

Following the filing of a Confidential Report of Concern, the Privacy Officer, or designee, shall investigate, and will complete the Investigation Report, attached hereto.

C. Non-Retaliation. Covered Entity will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against anyone for: (i) exercising any right under, or participating in any process established by the Privacy Rule or this Policy; (ii) filing a complaint with the Privacy Officer and/or the Department of Health and Human Services; (iii) testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or (iv) opposing in good faith any act or practice made unlawful by the Privacy Rule, provided that the manner of the opposition is reasonable and does not itself involve disclosure of PHI in violation of the applicable law.

INSTRUCTIONS RELATED TO COMPLAINTS

If a complaint is ever received, verbally or in writing, the complainant should be provided a copy of the attached Complaint Form. The completed form, or if the complaint is verbal, the information, shall be immediately provided to the Privacy Officer.

SEE ATTACHED CONFIDENTIAL REPORT OF CONCERN FORM FOR WORKFORCE OR AGENTS, SEE ATTACHED INVESTIGATION REPORT FORM, SEE ATTACHED COMPLAINT FORM FOR INDIVIDUALS

CONFIDENTIAL REPORT OF CONCERN

The purpose of this form is to report the facts pertaining to any known or suspected violation of the Covered Entity's privacy standards or the laws and regulations governing the Covered Entity. Although we ask you to provide your name, it is not necessary for you to do so if you wish to make an anonymous report. An anonymous report can be made by completing this form and mailing it to the Privacy Officer at the Covered Entity. If you do not want to give your name, you may call the Privacy Officer within one week of submitting this report to inquire about the outcome of the investigation.

If you wish to identify yourself in this report, the Covered Entity will make every effort to keep your identity confidential, unless you give the Covered Entity permission to reveal it. Only the Privacy Officer, and others designated by the Privacy Officer, will have access to your report. No disciplinary action or retaliation will be taken against you for making a good faith report of a compliance violation.

Please include all the factual details of the suspected violation, however big or small, to ensure that the Privacy Officer has all of the information necessary to conduct a thorough investigation. Please attach additional pages as needed. The information that you provide should include names, dates, times, places and a detailed description of the incident that led you to believe that a violation of the Covered Entity's privacy standards occurred. Please include a copy or a description of any documents that support your concerns.

Date of this report:

Name of person making this report (optional):

Description of the violation(s):

Detailed description of the incident(s) resulting in the violation (include names, dates, times and places):

Name(s) of person(s) involved in the incident and an explanation of their role:

Name(s) of other person(s) having knowledge of the incident:

Department where the incident occurred:

Date(s) of the incident:

Explanation of how you became aware of the suspected violation:

Please attach or describe any documents that support your concern (include a description of the documents, the identity of the persons who wrote the documents, the dates of the documents, and the location of the documents).

COMPLIANCE REPORT OF CONCERN INVESTIGATION

Date of reported concern:

Name of person who received the report:

Name of person who made the report (state “unknown” if the report was made anonymously):

Date(s) of investigation:

Name(s) of person(s) investigating: _____

Name(s) of person(s) interviewed: _____

Description of documents reviewed: _____

Findings:

Plan of correction:

_____

Privacy Officer

HEALTH PRIVACY COMPLAINT FORM

Today's Date: _____
Your Name: _____
Your Address: _____
_____
_____

Your Telephone Number:(___) ____–_____

Your Date of Birth: _____

Name of Entity you are complaining about: _____

Please describe the acts or omissions that you believe to be a violation of your privacy rights under privacy laws (attach additional sheets as necessary):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Date(s) that the above described acts or omissions occurred:

Please submit this complaint form to us at the following address:

_____
_____
_____
Attn: Privacy Officer

Thank you for taking the time to provide us with this information. You also have the right to file your complaint with the Secretary of the Department of Health and Human Services.

DE-IDENTIFIED INFORMATION AND RE-IDENTIFICATION POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individuals' PHI. Federal law allows use and disclosure of PHI for the purpose of creating de-identified information. De-identified information is information which has been stripped of any elements that may identify an Individual, such as name, birth date or social security number. Covered Entity may, from time to time, use de-identified data for various purposes. In doing so, Covered Entity will ensure that the appropriate administrative and technical processes are in place to properly de-identify PHI, as well as to secure any methods of re-identification, as required by the Privacy Rule and other applicable federal, state and/or local laws and regulations.

II. PURPOSE

The purpose of this policy is to provide guidance and ensure compliance with provisions of the Privacy Rule related to the de-identification of PHI.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.514

IV. PROCEDURE

A. De-Identified Information. Health information that does not identify an Individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an Individual is not Individually identifiable health information and therefore is not considered PHI under HIPAA. As such, it may be used or disclosed by Covered Entity without Authorization and for a purpose other than treatment, payment or health care operations, as long as the procedures set forth below are followed.

B. Requirements for De-Identification of PHI. Health Information may be deemed de-identified only under very specific circumstances, in accordance with the Privacy Rule.

1) The Privacy Officer shall make all decisions about whether PHI should be de-identified or if information received from another entity qualifies as de-identified information.

2) Information may be considered de-identified only if the following elements are removed or otherwise concealed from the PHI, and when the Covered Entity does not have actual knowledge that the information could be used along or in combination with other information to identify an Individual who is a subject of the information:

   a) name;
   b) all elements of dates (except year) for dates directly related to an Individual, including: birth date, date of death, all ages over 89; all elements of dates (including year) indicative of age 89, except that such ages and elements may be aggregated into a single category of age 90 or older;

c) telephone number;
d) fax number;
e) electronic mail address;
f) social security number;
g) medical record number;
h) health plan beneficiary number;
i) account number;
j) certificate/license number;
k) vehicle identifiers and serial numbers, including license plates;
l) device identifiers and serial number;
m) web Universal Resource Locators (URL);
n) Internet Protocol (IP) address number;
o) biometric identifiers, including finger and voice prints;
p) full face photographic image and any comparable image;
q) all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code or equivalent geocode; and
r) any other unique identifying number, characteristic or code, other than a code assigned to a record to permit Covered Entity to re-identify the information.
s) The initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census:

i. the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
ii. the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

3) Covered Entity shall adopt a uniform process for purposes of removing identifying elements from PHI.

4) If any of the identifiers listed above are not removed, then the information will only be disclosed when the Privacy Officer determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an Individual who is a subject of the information, and documents the methods and results of the analysis that justify that determination.

C. Re-identification. A Covered Entity may assign a code or other means of record identification to allow information that is de-identified under this Policy to be re-identified by the Covered Entity, as long as the following standards are met:

1) The code or other means of record identification used to re-identify information will not be derived from or related to information about the Individual and should not otherwise be capable of being translated so as to identify the Individual; and

2) The Covered Entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

LIMITED DATA SET POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individuals' PHI. For most disclosures other than in the usual course of treatment, payment, or health care operations, Covered Entity must obtain the Individual's Authorization before using or disclosing the Individual's PHI. However, Covered Entity may create and use a limited data set under certain circumstances. A limited data set contains information from which all direct identifiers, such as name, have been removed, but which may contain some indirect identifiers. Covered Entity will, from time to time, use or disclose limited data sets for purposes of research, public health and health care operations.

II. PURPOSE

The purpose of this policy is to provide guidance and to ensure that the creation, use and disclosure of limited data sets are in compliance with all applicable laws and regulations.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.514(e)

IV. PROCEDURE

A. General Rule Regarding Use or Disclosure of PHI for Purposes Other Than Treatment, Payment or Health Care Operations. Under the Privacy Rule, Covered Entity may not disclose an Individual's PHI for purposes other than treatment, payment or health care operations or other permitted uses and disclosures without obtaining the Individual's prior written Authorization.

B. Exceptions to General Rule. In some situations, Covered Entity may create de-identified information or limited data sets from PHI, without an Individual's Authorization, provided all of the requirements of the Privacy Rule have been met.

C. General Requirements for the Use or Disclosure of PHI to Create a Limited Data Set. Covered Entity may use PHI to create, or may disclose PHI to a Business Associate to create, a limited data set for the purposes of research, public health or health care operations. The following guidelines apply to the use or disclosure of PHI for the creation, use and disclosure of a limited data set:

1) The reason for creating and/or disclosing a limited data set must be documented and maintained. The Privacy Officer shall be consulted prior to the creation and/or disclosure of a limited data set.

2) The following Individually identifying elements of an Individual, relatives, employers and household providers of the Individual will be removed or otherwise excluded from PHI in order to create a limited data set:
   a) name;
   b) postal address information, other than town or city, state and zip code;
   c) telephone number;

d) fax number;
e) electronic mail address;
f) social security number;
g) medical record number;
h) health plan beneficiary number;
i) account number;
j) certificate/license number;
k) vehicle identifiers and serial numbers, including license plates;
l) device identifiers and serial number;
m) web Universal Resource Locators (URL);
n) Internet Protocol (IP) address number;
o) biometric identifiers, including finger and voice prints; and
p) full face photographic image and any comparable image.

3) Covered Entity will adopt processes for purposes of removing identifying elements from PHI to create a limited data set.

4) Covered Entity must enter into a data use agreement with any proposed recipients of a limited data set before disclosing any information contained in such limited data set to the recipient. This agreement must be reviewed by the Privacy Officer prior to use.

5) If Covered Entity is in receipt of a limited data set, Covered Entity will enter into and comply with the terms of a data use agreement. If the person or entity sending the limited data set to Covered Entity has not provided such an agreement, Covered Entity shall not use or disclose the information and shall promptly notify the Privacy Officer. If a data use agreement accompanies a limited data set received by Covered Entity, the employee will promptly forward the agreement to the Privacy Officer.

6) The data use agreement between Covered Entity and any other entity with which it will share the information contained in the limited data set, shall establish:

a) Who is permitted to use or receive the limited data set; and
b) The permitted uses and disclosures of such information by the recipient consistent with the limited purposes of research, public health and health care operations.

7) The data use agreement shall provide Covered Entity with adequate assurances that the recipient of the limited data set will:

a) Not attempt to re-identify or contact the Individuals whose information is contained in the limited data set;
b) Use appropriate safeguards to prevent uses or disclosures outside the terms of the data use agreement;
c) Ensure that any subcontractors or other tertiary recipients of the data agree to and abide by the terms of the data use agreement; and
d) Report any breaches of information or agreement to Covered Entity in a timely manner.

DATA USE AGREEMENT

This DATA USE AGREEMENT contract is between Central Iowa Community Services ("Covered Entity), and _____ ("Recipient") located at _____.

RECITALS

This Data Use Agreement is intended to comply with the requirements of the federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R Parts 160-164) ("HIPAA"). Pursuant to HIPAA, Covered Entity and Recipient are required to enter into a data use agreement to set forth the terms and conditions upon which Covered Entity will provide Recipient with access to, and Recipient will use, for purposes of research, public health, and healthcare operations, the Covered Entity's limited data set(s) (the "Limited Data Set"); and

The Health Information Technology for Economic and Clinical Health Act ("HITECH") was adopted as part of the American Recovery and Reinvestment Act of 2009. HITECH imposes new requirements with respect to privacy, security and breach notification and contemplates that such requirements be implemented in data use and business associate agreements.

NOW, THEREFORE, for and in consideration of the foregoing and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

I. LIMITED DATA SET

The Covered Entity's Limited Data Set contains only limited data set information as defined by HIPAA, 45 CFR 164.514 (e) (2).

II. USAGE GRANT

Covered Entity grants to the Recipient the use of the Limited Data Set as follows:

1) The Recipient shall use the Limited Data Set, and any backup/archival copies of the Limited Data Set, only for the purposes of research, public health, and healthcare operations in accordance with 45 CFR 164.514 (e)(3) and as set out in section III of this contract.

2) The Recipient may use the Limited Data Set for internal operations at the Recipient's places of business as permitted by this contract.

3) The Recipient may make backup/archival copies of the Limited Data Set, but shall not otherwise copy or transfer the Limited Data Set except as otherwise provided in this Contract.

4) The Recipient shall not license, rent, lease, or permanently transfer the Recipient's rights to the use the Limited Data Set to any other person except as otherwise provided in this Contract.

5) The Recipient shall maintain the confidentiality of the patient information contained in the Limited Data Set and shall not use or release data, directly or indirectly, either by act or by omission, in a manner which would result in the violation of the confidentiality of patient information. The Recipient shall ensure that any person using or receiving data from the Recipient does not violate patient confidentiality. The Recipient agrees to the following:

   a) Recipient will not use or further disclose the Limited Data Set other than as permitted by this Agreement, or as otherwise required by law;
   b) Recipient will use appropriate administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality and integrity of the Limited Data Set to prevent the use or disclosure of the Limited Data Set other than as provided for by this Agreement.
   c) Recipient will document and keep these safeguards current and available for inspection by Covered Entity upon request;
   d) Recipient will report to Covered Entity any use or disclosure of the Limited Data Set not provided for by this Agreement of which Recipient becomes aware within ten (10) days of becoming aware of the unauthorized use or disclosure. The report shall include (1) a description of all circumstances surrounding the unauthorized use or disclosure; and (2) the information in the Limited Data set that was used or disclosed in violation of this Agreement. Recipient shall cooperate as requested by Covered Entity in order to ascertain any additional facts that may be required to determine notification requirements;
   e) Recipient will ensure that any agents, including a subrecipient, to whom it provides the access to the Limited Data Set (if permitted by this agreement) agrees to the same restrictions and conditions that apply to Recipient with respect to the Limited Data Set;
   f) Recipient will not attempt to identify the individuals whose information is contained in the Limited Data Set or attempt to contact the individuals.

6) The Recipient shall not release from the Limited Data Set any grouping of data elements, in a report or other compilation of data, in which there are cells with three (3) or fewer records, unless the report or data compilation includes an asterisk or blank in a cell indicating that the case count is below the threshold for cell suppression. This shall not apply to the rule as of raw data by the Recipient provided that patient confidentiality is maintained by the person receiving the raw data.

III. RECIPIENT'S PURPOSE

The Recipient requests the data elements attached in Addendum A to be used consistent with paragraph II, 1. for the following exclusive purpose (s): [Insert Purposes]. The Recipient's request is limited to the minimum necessary data to accomplish the intended purpose of the request.

IV. ITEMS PROVIDED BY Covered Entity

Upon execution of this agreement and the payment of the fees specified in section V. of this Contract, Covered Entity shall provide the Recipient with a copy of the Limited Data Set in computer-readable form.

V. ITEMS PROVIDED BY RECIPIENT

In consideration for the use of the Limited Data Set, the Recipient agrees to pay _____.

All fee amounts payable under this Contract are exclusive of any taxes or other assessments, which are or may be due by reason of this Contract. The Recipient agrees to and shall pay any taxes or other assessments, which are or may be due by reason of this Contract.

VI. LIMITATIONS ON WARRANTIES

The Recipient accepts the Limited Data Set "As Is", "With All Faults", and without any warranties or conditions, express or implied, including, but not limited to, warranties for merchantability or fitness for a particular purpose or use.

Covered Entity is not responsible for the operation of the Limited Data Set, or any claim, loss, or injury resulting from operation or use of the Limited Data Set by the Recipient, including those of employees of the Recipient or third parties. The Recipient shall bear the entire risk and consequences of operation or use of the Limited Data Set, and shall bear all risk as to the quality of the data which results from that operation or use.

VII. TERM and TERMINATION

The terms of this Agreement shall be effective upon the Effective Date and shall continue until terminated by the parties in writing, or Covered Entity terminates the Agreement for a breach as described in this Section. In the event Covered Entity becomes aware of a material breach of Recipient's obligations with respect to use and disclosure of the Limited Data Set, Covered Entity may (1) provide an opportunity for Recipient to cure the breach or end the violation and terminate this Agreement in the event Recipient does not cure the breach or end the violation within the time specified by Covered Entity or (ii) immediately terminate this Agreement.

Upon termination of this Agreement for any reason, Recipient shall return or destroy all Limited Data Set information received by Recipient. This provision shall also apply to information that is in the possession of subrecipients or agents of Recipient. Recipient shall retain no copies of the information. In the event that return or destruction of the information is not feasible, Recipient shall provide to Covered Entity notification of the conditions that make return or destruction not feasible. In such case, Recipient shall extend the protections required under this Agreement and limit further uses and disclosures to those purposes that make the return or destruction not feasible, for as long as Recipient maintains such information.

VIII. DUTY TO DEFEND/INDEMNIFICATION

The Recipient shall defend Covered Entity against any claim, loss, or injury, including those of employees of the Recipient or third parties, which result directly or indirectly from the Recipient's operation of, or use or reliance upon, the Limited Data Set, including any use or

disclosure that does not comply with the restrictions of this Agreement. The Recipient shall indemnify Covered Entity against payment of any damages suffered by the Recipient, employees of the Recipient, or third parties, which arise directly or indirectly out of operation or use of, or reliance on, the Limited Data Set, whether or not the damages were disclosed to or reasonably foreseen by Covered Entity.

In the event of an actual or threatened breach by Recipient of the permitted uses and disclosures of the Limited Data Set information, Covered Entity shall be entitled to an injunction restraining and enjoining Recipient from violating the requirements of this Agreement. Nothing in this Agreement shall be construed as prohibiting Covered Entity from pursuing any other remedies available to Covered Entity for such breach or threatened breach, including the recovery of damages from Recipient and no remedy shall be considered exclusive. Recipient agrees to be responsible for and pay for any costs and expenses incurred by Covered Entity, including court costs and reasonable attorneys' fees, in the event that Covered Entity is required to enforce its rights under this Agreement.

IX. TRANSFERABILITY OF RIGHTS

Neither Covered Entity nor the Recipient may sell, transfer, assign, delegate, or subcontract any rights or obligations conveyed under this contract without the prior, express written consent of the other party. Any rights or obligations conveyed through a sale, transfer, assignment, delegation, or subcontract under this section shall be subject to the terms and conditions of this contract and the person purchasing, receiving, or assuming those rights or obligations shall be bound by the terms and conditions of this Contract.

X. CONTRACT MODIFICATION/SEVERABILITY

This Contract shall only be modified by the mutual written consent of the parties.

If any provision of this Contract is unlawful, void, or otherwise unenforceable, then that provision shall be severable from this Contract and shall not affect the validity or enforceability of the remaining provisions of this Contract.

XI. APPLICABLE LAW

This contract shall be construed and enforced in accordance with the laws of the State Iowa.

XII. ENTIRE AGREEMENT

This Agreement contains the entire agreement between Covered Entity and the Recipient regarding the Recipient's rights to access the Limited Data Set. Any previous understandings or agreements between Covered Entity and the Recipient regarding rights in or usage of the Limited Data Set, whether oral or written, are null and void as of the date of the signing of this contract.

XIII. ACKNOWLEDGMENT

The parties acknowledge that they have read the forgoing rights and obligations specified this Contract, and understand and agree to assume the rights and risks enumerated, including but not limited to all agreements to pay any fees or charges, disclaimers of warranty, limitations of liability, patient confidentiality requirements, and restrictions on transferability.

Signature of Recipient	Title/Position
Company	Date
Covered Entity	Date

GROUP HEALTH PLAN POLICY

I. POLICY

Covered Entity is committed to complying with HIPAA requirements related to group health plans. Group health plans are prohibited from disclosing PHI with their plan sponsor unless the group health plan ensures that the plan documents restrict uses and disclosures of PHI by the plan sponsor. This policy applies to the health care component of the Covered Entity that is a group health plan.

II. PURPOSE

The purpose of this policy is to ensure that the group health plan Covered Entity understands its obligations to amend its plan document related to uses and disclosures of PHI.

III. REFERENCES/CROSS-REFERENCES

- 45 CFR §164.504(f)

IV. PROCEDURE

A. General Rule. The Group Health Plan, in order to disclose PHI to the plan sponsor, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the following

1) *Summary Health Information*. The group health plan may disclose summary health information to the plan sponsor if the plan sponsor request the summary health information for the purpose of obtaining premium bids from health plans for providing health insurance coverage under the group health plan, or for the purpose of modifying, amending, or terminating the group health plan.

2) *Enrollment Information*. The group health plan may disclose to the plan sponsor information on whether the Individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

3) *Requirements for Amendment to Plan Documents*. The plan documents of the group health plan must be amended to incorporate provisions to:

   a) Establish the permitted and required uses and disclosures of PHI by the plan sponsor.
   b) Provide that the group health plan will disclose PHI to the plan sponsor only upon receipt of the certification by the plan sponsor that the plan documents have been amended to incorporate certain HIPAA-mandated provisions.
   c) Provide for adequate separation between the group health plan and the plan sponsor, including certain required provisions in the plan document amendment describing those classes of persons of the plan sponsor who have access to PHI, restricting the access to and use by such workforce

members, and providing an effective mechanism for resolving issues of noncompliance with the plan document amendment provisions required under HIPAA.

B. Uses and Disclosures. A group health plan may:

1) Disclose PHI to a plan sponsor to carry out plan administration functions that the plan sponsor performs, only consistent with the Amendment to Plan Documents described above, and attached hereto.

2) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose PHI to the plan sponsor except as permitted under HIPAA as described in this policy.

3) Not disclose (and may not permit a health insurance issuer or HMO to disclose) PHI to a plan sponsor in any event, unless certain required provisions are included in the notice of privacy practices.

4) Not disclose PHI to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

INSTRUCTIONS

1. The group health plan shall ensure that its plan document is amended to incorporate the HIPAA required provisions.

2. The group health plan shall ensure that it has received a signed certification from the plan sponsor that the plan document has been amended to incorporate the HIPAA required provisions.

Covered Entity is not a Health Plan.

MARKETING POLICY

I. POLICY

Covered Entity is committed to protecting the privacy of Individuals' PHI in compliance with all applicable laws and regulations. To achieve this commitment, Covered Entity has adopted a Privacy Program to help employees understand and recognize their responsibilities to protect the health information of Individuals, including in the context of the use of PHI for marketing purposes.

II. PURPOSE

The purpose of this Policy is to provide guidance regarding the privacy limitations on marketing communications and communications subsidized by manufacturers or other parties.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.501
- 45 C.F.R. §164.508(a)(3)

IV. PROCEDURE

A. Definition.

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing does not include a communication made:

1) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the Individual, only if any financial remuneration received in exchange for making the communication is reasonably related to the cost of making the communication. For purposes of this Marketing Policy, the term "financial remuneration" means direct or indirect payment from or on behalf of a third party whose product or service is being described.

2) For the following purposes, except where Covered Entity receives financial remuneration in exchange for making the communication:

   a) For treatment of an Individual, including case management or care coordination for the Individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the Individual;
   b) To describe a health-related product or service (or payment for such product or service) that is provided by Covered Entity; or
   c) For case management or care coordination, contacting of Individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

B. Marketing Restrictions

Covered Entity must obtain an Individual's authorization to use or disclose PHI for Marketing, except for face-to-face communications made by Covered Entity to the Individual, or for promotional gifts of nominal value. If Covered Entity would receive financial remuneration from a third party for the communication, the authorization must state that such remuneration is involved.

MINIMUM NECESSARY POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individual health information. While Individual information must be available to health care professionals in the process of ensuring proper care or other professional services, workforce members should avoid disclosing more Individual information than needed to perform our respective duties. To support our commitment to Individual confidentiality, the Covered Entity will ensure that the appropriate steps are taken to disclose only the minimum amount of PHI necessary to accomplish the particular use or disclosure, as required under HIPAA.

II. PURPOSE

The purpose of this policy is to provide employees with guidance on restricting the use and disclosure of PHI to the minimum necessary to achieve the purpose of the use or disclosure.

III. REFERENCE/CROSS-REFERENCE

- 45 C.F.R. §164.502(b)
- 45 C.F.R. §164.514(d)

IV. PROCEDURE

A. General Rule. The minimum necessary standard applies to all of Covered Entity's Uses and Disclosures of PHI except to (1) Disclosures to or requests by a health care provider when the PHI will be Used for Treatment purposes; (2) Disclosures to the Individual who is the subject of the PHI; (3) Uses or Disclosures made pursuant to an Authorization requested by the Individual; (4) Disclosures made to the Secretary under HIPAA; (5) Uses or Disclosures that are required by law under 45 CFR 164.512(a); and (6) Uses and Disclosures that are required for compliance with the Privacy Rule.

Covered Entity employees shall follow proper procedures to ensure that only the minimum amount of PHI necessary to accomplish the specific purpose of a use or disclosure is actually used or disclosed. Covered Entity employees shall request only the minimum amount of PHI necessary to accomplish the specific purpose of the request.

B. When Using or Disclosing PHI, or when requesting PHI from another entity, Covered Entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure or request for health information. Covered Entity must implement the following requirements after assessing their own unique circumstances. The requirements do not require limiting PHI Use or Disclosure to only what is absolutely the minimum necessary amount, but rather to what may reasonably be necessary to accomplish the purpose of the Use or Disclosure.

1) <u>Covered Entity personnel's access to PHI</u>. Covered Entity has identified those persons or classes of persons in its workforce who need access to PHI to carry out their duties. For each such person or class of persons, Covered Entity has identified the category or categories of PHI to which access is needed, and any appropriate

conditions to such access. Covered Entity must make reasonable efforts to limit the access to PHI of such identified persons or classes of persons to the identified categories of PHI. See Workforce Designation in this Manual.

2) Review of Requests. All proposed uses or disclosures of PHI shall be reviewed by persons having an understanding of the Covered Entity's privacy policies and practices, and sufficient expertise to understand and weigh the necessary factors.

3) Entire Record. The Covered Entity shall only use, disclose, or request an entire medical record when the entire medical record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.

4) Criteria. The following criteria will be used in limiting the amount of PHI requested or disclosed by Covered Entity's personnel:

Does the Individual who is requesting (disclosing) the PHI have complete understanding of the purpose for the use or disclosure of the PHI?

Are all of the Individuals identified for whom the requested use or disclosure of the PHI is required?

5) Minimum Necessary Disclosure of PHI.

a) For Disclosures made on a routine and recurring basis, Covered Entity must implement a standard protocol that limits the Disclosure to PHI reasonably necessary to achieve the purpose of the Disclosure.
b) For non-routine Disclosures, Covered Entity must develop criteria for determining and limiting such Disclosure to the minimum necessary PHI to accomplish the purpose of the non-routine Disclosure. Such Disclosures must be reviewed on a case by case basis in accordance with these criteria.

6) Minimum Necessary Requests for PHI.

a) For requests for PHI made on a routine and recurring basis, Covered Entity must implement a standard protocol that limits the Disclosure to PHI reasonably necessary to achieve the purpose of the Disclosure.
b) For non-routine requests, Covered Entity must develop criteria for determining and limiting Disclosure to the minimum necessary PHI to accomplish the purpose of the non-routine Disclosure. Such requests must be reviewed on a case by case basis in accordance with these criteria.

7) Reasonable Reliance. Covered Entity may rely on a requested Disclosure for PHI as being the minimum necessary for a stated purpose when the request is made by:

a) A public health official or agency for a Disclosure permitted under the Privacy Rule;
b) Another Covered Entity;
c) A professional who is a workforce member or Business Associate of the Covered Entity holding the PHI; or

d) A researcher with appropriate documentation from an Institutional Review Board or Privacy Board.

NOTICE OF PRIVACY PRACTICES POLICY

I. POLICY

Covered Entity shall comply with the Privacy Rule governing the provision of a Notice of Privacy Practices to Individuals seeking Covered Entity services and to health plan beneficiaries and new enrollees. As set forth in this Policy, Individuals have the right to adequate notice by Covered Entity of the uses and disclosures of their PHI permitted or required by Covered Entity, and of their rights and Covered Entity duties under HIPAA with respect to PHI. Further, Covered Entity shall make a good faith effort to obtain a written acknowledgement from each Individual seeking treatment or

II. PURPOSE

The purpose of this Policy is to ensure that Covered Entity complies with the rules governing the provision of a Notice of Privacy Practices, and to ensure that employees are familiar with the general rules concerning the timing and distribution of the Notice. Another purpose of this Policy is to provide guidance to employees about the process by which an acknowledgment of receipt of Covered Entity's Notice of Privacy Practices must be obtained from Individuals presenting for services and from beneficiaries and enrollees in the health plan.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.520

IV. PROCEDURE

V. Notice of Privacy Practices for Health Care Provider.

1) General Rules. Each Individual seeking health care from Covered Entity, except for inmates, must receive a Notice. If a material change is made to the Notice, the Notice shall be revised under the direction of the Privacy Officer and shall be redistributed according to the distribution of Notice provisions contained in this Policy.

2) Distribution of Notice.

   a) *General Rule*. Each Individual shall receive a Notice not later than the first date of service delivery, including service delivered electronically.

   b) *Electronic Distribution*. The Notice also shall be available electronically, for viewing only, through Covered Entity's web-site at https://www.cicsmhds.org/

   c) *Upon Request*. A paper copy of the Notice shall be provided upon request to any Individual seeking health care services from Covered Entity, regardless of whether the Individual has agreed to receive the Notice electronically.

   d) *Service Delivery Site*. If the Covered Entity maintains a physical service delivery site, the Covered Entity must have the Notice available at the service delivery site for Individuals to request to take with them and must post the Notice in a clear and prominent location where it is reasonable to

expect Individuals seeking services from Covered Entity to be able to read the Notice.

B. Notice of Privacy Practices for Health Plan

1) General Rule. To the extent required by the Privacy Rule, the Covered Entity Health Plan shall provide a Privacy Notice to Covered Employees. If a material change is made to the Privacy Notice, the Privacy Notice shall be revised under the direction of the Privacy Officer and shall be redistributed according to the distribution of Privacy Notice provisions of this Policy.

2) Distribution of Notice

a) Each Covered Employee enrolled in a Plan will receive a Privacy Notice. Covered spouses and dependents shall not be entitled to separate notification apart from what is provided to the Covered Employee, unless a copy of the Privacy Notice is requested by such Individual.

b) Privacy Notices shall be provided: (i) at the time of enrollment, to each newly eligible Covered Employee; and (ii) if the Privacy Notice is not posted on the Plan's website, within 60 days of a material revision of the Privacy Notice, or if the Privacy Notice is posted on the Plan's website, the change shall be posted on the website by the effective date of the change and the revised Privacy Notice shall be included in its next annual mailing to all then Covered Employees. Every three years each Covered Employee shall either (i) be informed that the Privacy Notice is available upon request and provided with directions as to how to obtain the Privacy Notice; or (ii) be provided with the Privacy Notice itself. The Privacy Notice also shall be available electronically to all Covered Employees.

c) The Privacy Notice may be distributed electronically at the discretion of the Plans, within the time frames provided above, if the following requirements are met: (i) the recipients have agreed in advance to receive the Notice electronically; and (ii) such agreement has not been withdrawn. To the extent Covered Entity has knowledge that an electronic transmission of the Privacy Notice has failed, a paper copy of the Privacy Notice shall be provided.

d) A paper copy of the Privacy Notice shall be provided upon request to any Individual enrolled in the Plan, regardless of whether the Individual has agreed to receive the Privacy Notice electronically.

C. Content of the Notice of Privacy Practices

1) Required Elements. The Covered Entity must provide a Notice that is written in plain language and that contains the following elements:

a) Header: "This Notice Describes How Medical Information About You May Be Used and Disclosed and How You Can Get Access to This Information. Please Review It Carefully."

b) A description, including at least one example, of the types of uses and disclosures that the Covered Entity is permitted to make for treatment, payment and health care operations.

c) A description of each of the other purposes for which the Covered Entity is permitted to use or disclose PHI without the Individual's written authorization.

d) If a use or disclosure is prohibited or materially limited by other applicable law, the description of the use or disclosure shall reflect the more stringent law.

e) A description of the types of uses and disclosures that require an authorization under the HIPAA provisions governing psychotherapy notes, marketing and sales of PHI, a statement that other uses and disclosures not described in the Notice will be made only with the Individual's written authorization, and a statement that the Individual may revoke such authorization. If the Covered Entity contacts Individuals to remind them of appointments or to provide them with other information, the Covered Entity shall describe that on the notice.

f) A statement of the Individual's rights with respect to PHI and a brief description of how the Individual may exercise these rights.

   i. The right to request restrictions on certain uses and disclosures and that the Covered Entity is not required to agree to a requested restriction except in the case of mandatory disclosure restrictions to health plans when the Individual paid for the cost of the service in full.
   ii. The right to receive confidential communications of PHI.
   iii. The right to inspect and copy PHI.
   iv. The right to amend PHI.
   v. The right to receive an accounting of PHI disclosures.
   vi. The right to obtain a paper copy of the notice from the Covered Entity.

g) A statement that the Covered Entity is required to maintain the privacy of PHI and to provide the Individual with notice of its legal duties and privacy practices with respect to PHI, and to notify the Individual following a breach of unsecured PHI.

h) A statement that the Covered Entity is required to abide by terms of the notice currently in effect.

i) A statement that the Covered Entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains. The statement shall also describe how it will provide Individuals with the revised notice.

j) A statement that the Individual may complain to the Covered Entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the Individual may file a complaint and a statement that the Individual will not be retaliated against for filing a complaint.

k) The name or title and telephone number of the person or office to contact for further information.

l) A date on which the notice is first in effect.

2) Optional Elements. If the Covered Entity intends to engage in any of the following, the Notice must include a separate statement informing the Individual of such activities, as follows:

a) If the Covered Entity engages in fundraising activities, a statement that the Covered Entity may contact the Individual to raise funds for the Covered Entity and the Individual has a right to opt out of receiving such communications.

b) A group health plan may disclose PHI to the sponsor of the plan.

c) A health plan that intends to use of disclose PHI for underwriting purposes must include a statement that the Covered Entity is prohibited from using or disclosing PHI that is genetic information of an Individual for such purposes.

D. Obtaining Acknowledgement of Receipt of Notice for Health Care Providers

1) General Rule. Covered Entity must make a good faith effort to obtain an Individual's acknowledgment that he or she has received the Notice no later than the first date of service delivery.

2) Exceptions. In emergency situations, Covered Entity may wait to obtain the acknowledgment until reasonably practicable.

3) Refusal. If an Individual refuses or otherwise fails to provide an acknowledgment, Covered Entity must document its good faith effort to obtain the acknowledgment and the reason why the acknowledgment was not obtained (e.g., the Individual refused to sign the acknowledgment after being requested to do so). Covered Entity is not prohibited from providing treatment or otherwise using or disclosing PHI as permitted by law if the Individual does not sign an acknowledgment after being asked to do so.

4) One Acknowledgment. Covered Entity only needs to obtain one signed acknowledgment per Individual. Covered Entity is not required to collect an acknowledgment every time the Individual obtains services. Even if Covered Entity's Notice is revised, Covered Entity is not required to ask the Individual to sign a new acknowledgment.

5) Process for Obtaining Acknowledgments. Covered Entity shall provide each Individual seeking treatment from Covered Entity with a Notice on the first date of service. Each Individual must be provided with a paper copy to take with them if requested.

a) Employees of Covered Entity, after providing the Individual an opportunity to review the Notice, shall request that the Individual sign the

acknowledgment, which shall be captured by electronic or manual signature for documentation purposes.

b) If an Individual refuses to sign an acknowledgment after having been asked to do so, the employee must document the refusal and the reason for the refusal using Covered Entity's designated form, and forward the refusal to Covered Entity's Privacy Officer.

6) Separate Signature Requirement. If Covered Entity is required to collect an Individual signature for another purpose, the signature obtained for the acknowledgment must be separate and the language must indicate the Individual knows what he or she is signing.

SEE ATTACHED TEMPLATE NOTICE OF PRIVACY PRACTICES FOR HEALTH CARE PROVIDER; SEE ATTACHED TEMPLATE NOTICE OF PRIVACY PRACTICES FOR HEALTH PLAN; SEE ATTACHED ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES FOR HEALTH CARE PROVIDER; SEE ATTACHED GOOD FAITH EFFORT TO OBTAIN ACKNOWLEDGMENT OF RECEIPT FOR HEALTH CARE PROVIDER

NOTICE OF PRIVACY PRACTICES FOR HEALTH CARE PROVIDERS

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

If you have any questions about this Notice of Privacy Practices, contact the Covered Entity's Privacy Officer:

Russell Wood
russell.wood@cicsmhds.org
641-456-2128
123 1st Ave SW (PO Box 58)
Hampton, IA 50441

This Notice of Privacy Practices describes how the Covered Entity may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information ("PHI"). "PHI" is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services.

The Covered Entity is required to abide by the terms of this Notice of Privacy Practices. The Covered Entity may change the terms of this notice, at any time. The new notice will be effective for all PHI that the Covered Entity maintains at that time. Upon request, the Covered Entity will provide you with any revised Notice of Privacy Practices.

PERMITTED USES AND DISCLOSURES OF PHI

Your PHI may be used and disclosed by the Covered Entity for the purpose of providing or accessing health care services for you. Your PHI may also be used and disclosed to pay your health care bills and to support the business operation of the Covered Entity.

The following categories describe ways that the Covered Entity is permitted to use and disclose health care information. Examples of types of uses and disclosures are listed in each category. Not every use or disclosure for each category is listed; however, all of the ways the Covered Entity is permitted to use and disclose information falls into one of these categories:

1) Treatment:
The Covered Entity may use and disclose your PHI to provide, coordinate or manage your health care and any related services. This includes the coordination or management of your health care with a third party that has already obtained your permission to have access to your PHI. For example, the Covered Entity would disclose your PHI, as necessary, to a home health agency that provides care to you. Another example is that PHI may be provided to a facility to which you have been referred to ensure that the facility has the necessary information to treat you.

2) Payment
The Covered Entity may use and disclose health care information about you so that the treatment and services you receive may be billed to and payment may be collected from you, an insurance

company or a third party. The Covered Entity may also discuss your PHI about a service you are going to receive to determine whether you are eligible for the service, and for undertaking utilization review activities. For example, authorizing a service may require that your relevant PHI be discussed with a provider to determine your need and eligibility for the service.

3) **Healthcare Operations**

The Covered Entity may use or disclose, as-needed, your PHI in order to support its business activities. These activities include, but are not limited to, quality assessment activities, employee review activities, licensing and conducting or arranging for other business activities. For example, the Covered Entity may use or disclose your PHI, as necessary, to contact you to remind you of your appointment or to provide information about alternate services or other health-related benefits.

The Covered Entity may share your PHI with third party "business associates" that perform various activities (e.g., billing, transcription services) for the Covered Entity. Whenever an arrangement between the Covered Entity and a business associate involves the use or disclosure of your PHI, the Covered Entity will have a written contract that contains terms that will protect the privacy of your PHI.

USES AND DISCLOSURES OF PHI REQUIRING YOUR WRITTEN AUTHORIZATION

Other uses and disclosures of your PHI will be made only with your written authorization, unless otherwise permitted or required by law as described below. You may revoke this authorization, at any time, in writing, except to the extent that the Covered Entity has taken an action in reliance on the use or disclosure indicated in the authorization.

The Covered Entity also may keep psychotherapy notes. These are given a higher degree of protection and cannot be disclosed without your express permission except to carry out certain treatment, payment, or health care operations including allowing the note taker to use them for treatment, using the notes for training programs, or using the notes in defense of a legal proceeding. You have the opportunity to specifically authorize disclosure of psychotherapy notes on the *Authorization for Release of PHI* form.

We will not use or disclose your PHI for marketing purposes without your written authorization unless the marketing is conducted through a face-to-face communication or involves a gift of nominal value.

We will not accept payment of any kind for your PHI without your written authorization. Sale of PHI is prohibited only as it is defined by law and does not include accepting payment for your treatment.

You may revoke an authorization at any time by notifying us in writing. If this should ever be the case, please be aware that revocation will not impact any uses or disclosures that occurred while the authorization was in effect.

The Covered Entity may use and disclose your PHI in the following instances. You have the opportunity to agree or object to the use or disclosure of all or part of your PHI. If you are not present or able to agree or object to the use or disclosure of the PHI, then the Covered Entity may,

using professional judgment, determine whether the disclosure is in your best interest. In this case, only the PHI that is relevant to your health care will be disclosed.

1) **Others Involved in Your Healthcare**

Unless you object, the Covered Entity may disclose to a member of your family, a relative, a close friend or any other person you identify, your PHI that directly relates to that person's involvement in your health care. If you are unable to agree or object to such a disclosure, the Covered Entity may disclose such information as necessary if the Covered Entity, based on its professional judgment, determines that it is in your best interest. The Covered Entity may use or disclose PHI to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location, general condition or death. Finally, the Covered Entity may use or disclose your PHI to an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other Individuals involved in your health care.

2) Emergencies

The Covered Entity may use or disclose your PHI in an emergency treatment situation. If this happens, the Covered Entity shall try to obtain your acknowledgment of receipt of the Notice of Privacy Practices as soon as reasonably practicable after the delivery of treatment.

OTHER PERMITTED AND REQUIRED USES AND DISCLOSURES THAT MAY BE MADE WITHOUT YOUR AUTHORIZATION OR OPPORTUNITY TO OBJECT

The Covered Entity may use or disclose your PHI in the following situations without your consent or authorization. These situations include:

1) Required By Law

The Covered Entity may use or disclose your PHI to the extent that the law requires the use or disclosure. You will be notified, as required by law, of any such uses or disclosures.

2) Public Health

The Covered Entity may disclose your PHI for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. The disclosure will be made for the purpose of controlling disease, injury or disability. The Covered Entity may also disclose your PHI, if directed by the public health authority, to a foreign government agency that is collaborating with the public health authority.

3) Communicable Diseases

The Covered Entity may disclose your PHI, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease.

4) Health Oversight

The Covered Entity may disclose your PHI to a health oversight agency for activities authorized by law, such as audits, investigations and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

5) Abuse or Neglect

The Covered Entity may disclose your PHI to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, the Covered Entity may disclose your PHI if it believes that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

6) Food and Drug Administration

The Covered Entity may disclose your PHI to a person or company required by the Food and Drug Administration to report adverse events, product defects or problems, biologic product deviations, track products; to enable product recalls; to make repairs or replacements, or to conduct post marketing surveillance, as required.

7) Legal Proceedings

The Covered Entity may disclose PHI in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), in certain conditions in response to a subpoena, discovery request or other lawful process.

8) Law Enforcement

The Covered Entity may also disclose PHI, so long as applicable legal requirements are met, for law enforcement purposes. these law enforcement purposes include (1) legal processes and otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on Covered Entity premises, and (6) medical emergency (not on the Covered Entity's premises) and it is likely that a crime has occurred.

9) Coroners, Funeral Directors, and Organ Donation

The Covered Entity may disclose PHI to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose PHI to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We may disclose such information in reasonable anticipation of death. PHI may be used and disclosed for cadaveric organ, eye or tissue donation purposes.

10) Research

The Covered Entity may disclose your PHI to researchers when their research has been approved by an Institutional Review Board that has reviewed the research proposal and established protocols to ensure the privacy of your PHI.

11) Criminal Activity

Consistent with applicable federal and state laws, the Covered Entity may disclose your PHI, if it believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. The Covered Entity may also disclose PHI if it is necessary for law enforcement authorities to identify or apprehend an Individual.

12) Military Activity and National Security

When the appropriate conditions apply, the Covered Entity may use or disclose PHI of Individuals who are Armed Forces personnel (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veterans Affairs

of your eligibility for benefits, or (3) to foreign military authority if you are a member of that foreign military service. The Covered Entity may also disclose your PHI to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

13) Workers' Compensation
Your PHI may be disclosed by the Covered Entity as authorized to comply with workers' compensation laws and other similar legally established programs.

14) Inmates
The Covered Entity may use or disclose your PHI if you are an inmate of a correctional facility and the Covered Entity created or received your PHI in the course of providing care to you.

15) Required Uses and Disclosures
Under the law, the Covered Entity shall make disclosures to you and when required by the Secretary of the Department of Health and Human Services to investigate or determine the Covered Entity's compliance with the requirements of 45 C.F.R. section 164.500 et. seq.

YOUR RIGHTS

The following are a list of your rights with respect to your PHI and a brief description of how you may exercise these rights:

RIGHT TO INSPECT AND COPY YOUR PHI

This means you may inspect and obtain a copy of PHI about you that is contained in a designated record set for as long as the Covered Entity maintains the PHI. A "designated record set" contains medical and billing records and any other records that the Covered Entity uses in making decisions about you.

Under federal law, however, you may not inspect or copy the following records; psychotherapy notes; information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding, and PHI that is subject to law that prohibits access to PHI. Depending on the circumstances, a decision to deny access may be reviewable. In some circumstances, you may have a right to have this decision reviewed. Please contact the Covered Entity Privacy Officer if you have questions about access to your medical record.

RIGHT TO REQUEST A RESTRICTION OF YOUR PHI

This means you may ask the Covered Entity not to use or disclose any part of your PHI for the purposes of treatment, payment or healthcare operations. You may also request that any part of your PHI not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. Your request must state the specific restriction requested and to whom you want the restriction to apply.

The Covered Entity is not required to agree to a restriction that you may request, except in the case of a disclosure you have restricted under 45 C.F.R. §164.522(a)(1)(vi) related to restricted disclosures to health plans if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law, and the PHI pertains solely to a health care item or service for which you have (or someone other than you but not the health plan has) paid

out-of-pocket, in full. If the Covered Entity believes that it is in your best interest to permit use and disclosure of your PHI, your PHI will not be restricted. If the Covered Entity does agree to the requested restriction, it may not use or disclose your PHI in violation of that restriction unless it is needed to provide emergency treatment. With this in mind, please discuss any restriction you wish to request with the Covered Entity. You may request a restriction in writing to the Covered Entity Privacy Officer. To request a restriction, you must provide us, in writing 1) what information you want to limit; 2) whether you want to limit our use, disclosure or both; and 3) to whom you want the limits to apply.

RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS FROM THE COVERED ENTITY BY ALTERNATIVE MEANS OR AT AN ALTERNATIVE LOCATION

The Covered Entity will accommodate reasonable requests. The Covered Entity may also condition this accommodation by asking you for information as to how payment will be handled or specification of an alternative address or other method of contact. The Covered Entity will not request an explanation from you as to the basis for the request. Please make this request in writing to the Covered Entity Privacy Officer.

RIGHT TO REQUEST AN AMENDMENT TO YOUR PHI

This means you may request an amendment of PHI about you in a designated record set for as long as the Covered Entity maintains this information. In certain cases, the Covered Entity may deny your request for an amendment. If the Covered Entity denies your request for amendment, you have the right to file a statement of disagreement with the Covered Entity and the Covered Entity may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal. All requests for amendments must be in writing.

RIGHT TO RECEIVE AN ACCOUNTING OF CERTAIN DISCLOSURES OF YOUR PHI

This right applies to disclosures for purposes other than treatment, payment or healthcare operations as described in this Notice of Privacy Practices. It excludes disclosures the Covered Entity may have made to you, to family members or friends involved in your care, or for notification purposes. You have the right to receive specific information regarding these disclosures that occur after April 14, 2003.

RIGHT TO OBTAIN A PAPER COPY OF THIS NOTICE

You have the right to obtain a paper copy of this notice, upon request, even if you have agreed to accept this notice electronically.

THE COVERED ENTITY'S DUTIES AND OTHER INFORMATION

The Covered Entity is required by law to maintain the privacy of PHI and to provide you with this notice of our legal duties and privacy practices with respect to PHI, and abide by the terms of the notice currently in effect.

We must inform you of any breach of your PHI that compromises your PHI and that is held or transmitted in an unsecured manner, within 60 days after we discover, or by exercising reasonable diligence, should have discovered the breach.

We reserve the right to change our policies and practices regarding how we use or disclose PHI, or how we will implement Individual rights concerning PHI. We reserve the right to change this notice and to make the provisions in our new notice effective for all information we maintain. If we change these practices, we will publish a revised Notice of Privacy Practices. The revised notice will be posted and available at our places of service.

COMPLAINTS

You may file a complaint to the Covered Entity or to the Secretary of Health and Human Services if you believe your privacy rights have been violated by the Covered Entity. You may file a complaint against the Covered Entity by notifying the Covered Entity Privacy Officer. The Covered Entity will not retaliate against you for filing a complaint.

You may contact the Covered Entity Privacy Officer,

Russell Wood
russell.wood@cicsmhds.org
641-456-2128
123 1st Ave SW (PO Box 58)
Hampton, IA 50441
for further information about the complaint process.

This notice was published and becomes effective on 7/1/2022.

ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICE FOR HEALTH CARE PROVIDERS

I, _____, do hereby acknowledge receipt of a copy of the Notice of Privacy Practice, Policy and Procedure.

_____

Signature of Individual

_____

Date

IN THE EVENT THIS NOTICE IS RECEIVED BY THE INDIVIDUAL'S PERSONAL REPRESENTATIVE

_____

Signature of personal representative Date

_____

Legal authority of personal representative

"GOOD FAITH EFFORT" TO GAIN ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICE FOR HEALTH CARE PROVIDERS

This is an acknowledgement of a good faith effort in regards to the following client:

Client Name ID #

A copy of the Notice of Privacy Practices has not been given to the Individual for the reason(s) stated below:

_____

_____

_____

A copy of the Notice of Privacy Practices has been given to the Individual but receipt was not obtained for the reason(s) stated below:

_____

_____

_____

_____

Employee Signature Date

☐ Certified Mail Return Receipt Attached

PRIVACY OFFICER DESIGNATION POLICY

I. POLICY

In order to manage the facilitation and implementation of activities related to the privacy and security of PHI, Covered Entity has appointed and will maintain a Privacy Officer position.

The Privacy Officer will be responsible and shall serve as the focal point for all privacy compliance-related activities. In general, the Privacy Officer is charged with implementing Covered Entity's HIPAA Privacy Policies and Procedures, conducting educational programs, and administering reviews relating to privacy and confidentiality Policies and Procedures.

Russell Wood has been designated the Privacy Officer of Covered Entity.

II. PURPOSE

The purpose of this Policy is to set forth the responsibilities of the Privacy Officer.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.530(a)

IV. PROCEDURE

A. General Rule. The Privacy Officer must demonstrate familiarity with the legal requirements relating to privacy and health care operations, as well as the ability to communicate effectively with and coordinate the efforts of medical, technical, management and clerical personnel.

B. Responsibilities. The Privacy Officer:

1) Provides leadership to the Covered Entity's committees, work groups, and task forces charged with creating and implementing an enterprise-wide privacy program.

2) Develops Covered Entity's privacy Policies and Procedures consistent with applicable laws, rules, and regulations.

3) Ensures that processes are implemented to maintain compliance with Federal and State laws related to privacy, security, confidentiality, and protection of information resources and health care information. This includes coordination with the Security Officer in evaluating and monitoring operations and systems development for security and privacy requirements.

4) Develops, implements, and administers Covered Entity's authorization procedures for access to, use, and disclosure of PHI.

5) Develops, implements, and administers a Covered Entity procedure to allow Individuals to exercise their rights to PHI under applicable State and Federal Laws.

6) Develops and implements Covered Entity's privacy training programs and, in conjunction with the Security Officer, a security awareness and training program.

7) Coordinates with the other leaders, such as a compliance officer and human resources staff to develop appropriate sanctions for employees or business partners that fail to comply with the Covered Entity's privacy Policies and Procedures.

8) Coordinates with other Covered Entity programs to measure effectiveness, performance and quality of the Covered Entity's privacy program.

9) Coordinates with other leaders such as a compliance officer regarding complaints and information relating to the Covered Entity's privacy program and regarding investigation of all allegations of non-compliance with the Covered Entity's privacy Policies.

10) Coordinates with the Security Officer and other applicable leaders and departments regarding the mitigation of the effects of any unauthorized or otherwise inappropriate released of health information.

11) On a periodic basis reports the status of the privacy program to the Board or other governance body.

12) Serves as resource to the Covered Entity's designated liaisons to regulatory and accrediting bodies for matters relating to privacy and security.

SAFEGUARDS POLICY

I. POLICY

Covered Entity shall implement reasonable and appropriate administrative, technical and physical safeguards to protect the privacy of PHI.

II. PURPOSE

The purpose of this Policy is to ensure that Covered Entity complies with rules governing the Use or Disclosure of PHI, and to ensure that Covered Entity workforce members are familiar with the general rules.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.530(c)

IV. PROCEDURE

Covered Entity's protocol for safeguarding PHI takes into account Covered Entity's computer equipment and computer security options, physical layout, staffing level and Individual population, in order to protect, to the greatest extent possible, any incidental Uses and Disclosures of PHI that could occur. The protocol will be based on the following principles:

A. General Rule. PHI may be Used or Disclosed only as allowed by the Privacy Rule, regardless of whether that Use or Disclosure occurs in person, electronically or through a workstation.

B. Workstation. Covered Entity may Use or Disclose PHI by way of a workstation only in a manner that reasonably safeguards the PHI from unintentional Disclosure to or Use by anyone other than the intended user or recipient. Reasonable safeguards may include:

1) Ensuring that workstations are not positioned in a manner that allows others to easily view the workstation screen.

2) Ensuring that workstations are equipped with password protection and other reasonable security measures so that unauthorized persons cannot access PHI on an unattended workstation or through Covered Entity's server or network; and

3) Restricting access to the workstations to the designated Covered Entity workforce who have a legitimate need to have such access.

C. Oral Communications. Covered Entity staff shall use reasonable safeguards to protect Individual privacy during all interactions with Individuals or other Individuals, related to PHI. The safeguards Covered Entity staff use shall be tailored to the particular facts and circumstances of each interaction, depending on the physical layout of Covered Entity, the proximity to other Individuals in the area, the content of the interaction with the Individual, and other conditions or circumstances that may affect the privacy of Covered Entity workforce interactions regarding PHI. It is the responsibility of each Covered Entity workforce member to determine, in each circumstance, the reasonable safeguards to

employ in order to protect Individual privacy to the greatest extent possible, while considering the potential effects on Individuals. Reasonable safeguards may include:

1) Keeping voices low during all interactions regarding PHI so that others cannot hear the conversation;

2) Taking steps to ensure that discussions involving PHI are not overheard. Persons will be trained on the following safeguards to protect oral communications: (i) conducting conversations in a room with a door if necessary, (ii) lowering speaking voice when discussing PHI, (iii) using the handset of the telephone instead of the speakerphone, (iv) when speaking to an Individual about PHI keeping a distance from surrounding Individuals; and (v) being sure to Disclose only the minimum necessary amount of PHI.

3) Persons will verify that the person with whom he or she is speaking is the actual Individual who is the subject of the PHI or the authorized representative of such Individual (e.g., requesting social security number or date of birth, or other identifying information).

4) Restricting the type and amount of information left on an Individual's home or work voicemail or answering machine.

D. Disposal of PHI. PHI must not be discarded in unsecured trash bins, unsecured bags or other publicly-accessible locations. Instead, all PHI, such as paper records including PHI and labeled prescription bottles, shall be discarded in secured trash receptacles or other non-publicly-accessible locations, or shredded, burnt, pulped, or pulverized so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

SALE OF PHI POLICY

I. POLICY

Covered Entity is committed to protecting the privacy and security of PHI and shall not, without the Individual's prior written authorization, exchange remuneration for an Individual's PHI.

II. PURPOSE

The purpose of this Policy is to ensure that Covered Entity workforce members are aware of the prohibition on the sale of PHI without an authorization from the Individual.

III. REFERENCE/CROSS-REFERENCE

- 45 C.F.R. §164.508(a)(4)

IV. PROCEDURE

A. General Rule. Except as set forth below, Covered Entity shall not directly or indirectly receive payment in exchange for PHI of an Individual unless the Individual provided to Covered Entity a valid authorization in accordance with 45 C.F.R. § 164.508 that specifically authorizes Covered Entity to exchange the PHI for payment.

B. Exceptions to Prohibition of Sale of PHI. Paragraph A above does not prohibit payment in exchange for PHI in the following circumstances:

1) The purpose of the exchange is for public health activities (as described in 45 C.F.R. § 164.512(b) or § 164.514(e)).

2) The purpose of the exchange is for research (pursuant to 45 C.F.R. § 164.514(e) or § 164.512(i)) and the payment received is a reasonable cost-based fee to cover costs of preparation and transmittal of the PHI for such purpose.

3) The purpose of the exchange is for the treatment of the Individual or for payment purposes pursuant to 45 C.F.R. § 164.506(a).

4) The purpose of the exchange is to facilitate the sale, transfer, merger, or consolidation of all or part of Covered Entity, and due diligence related to such activity.

5) The purpose of the exchange is for activities that a Business Associate undertakes on behalf of Covered Entity, and the payment is provided to the Business Associate solely for the performance of those activities.

6) The purpose of the exchange is to provide an Individual with a copy of the Individual's PHI pursuant to 45 C.F.R. § 164.524 or § 164.528.

7) The exchange is required by law as permitted under 45 C.F.R. § 164.512(a).

8) The exchange is for any other purpose permitted by the Privacy Rule when the only payment received is a reasonable, cost-based fee to cover costs of preparation and transmittal of the PHI for such purpose or a fee otherwise expressly permitted by law.

SANCTIONS POLICY

I. POLICY

Covered Entity has established and will apply appropriate sanctions against members of its workforce, as well as other agents and contractors, who fail to comply with its HIPAA policies and procedures.

II. PURPOSE

This Policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to sanctions for violating Covered Entity's HIPAA policies and procedures. Under the Privacy Rule, penalties for misuse or misappropriation of health information include both civil monetary penalties and criminal penalties.

Civil penalties range from $100 for each violation to a maximum of $1,500,000 per year for the same violations.

Criminal penalties vary from $50,000 and/or one year imprisonment to $250,000 and/or ten years imprisonment (42 U.S.C. §§ 1320d 5 and 1320d 6).

III. REFERENCE/CROSS-REFERENCE

- 45 C.F.R. §164.530(e)

IV. PROCEDURE

A. General Rule Regarding Sanction. All workforce members shall comply with the written policies and procedures included in this Privacy Manual as amended from time to time, and such compliance shall be a factor considered in each employee's evaluation. In addition, Covered Entity shall apply appropriate sanctions or discipline against every member of its workforce that fails to comply with Covered Entity's Policies and Procedures. Such sanctions or discipline shall be applied in compliance with Covered Entity's human resources policies and procedures and applicable collective bargaining agreements. The type and severity of the sanction applied shall depend on whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors. Sanctions could range from verbal reprimand to termination.

Employees, agents, and other contractors should be aware that violations may result in notification to law enforcement officials, Individuals whose PHI is inappropriately access, acquired, used or disclosed, as well as to regulatory, accreditation, and/or licensure organizations.

B. General Process for Responding to Possible Violations.

1) Members of Covered Entity's workforce are encouraged to report possible Privacy Violations to Covered Entity's Privacy Officer.

2) Whenever possible Privacy Violations arise, the Privacy Officer shall conduct an investigation and determine whether a violation has occurred.

3) A record of the event and any discipline imposed shall be maintained by the Privacy Officer.

C. Mitigation. The Covered Entity shall mitigate, to the extent practicable, any harmful effect known to the Covered Entity of a use or disclosure of PHI in violation of its policies and procedures by the Covered Entity workforce members or by its business associates.

D. Examples of HIPAA Violations Which May Result in Sanctions

- Accessing information that you do not need to know to do your job;
- Sharing your computer access codes (user name & password)/ Using another person's computer access codes (user name & password);
- Leaving your computer unattended while you are logged into a PHI program;
- Sharing PHI with another employee without authorization;
- Copying PHI without authorization;
- Changing PHI without authorization;
- Discussing confidential information in a public area or in an area where the public could overhear the conversation;
- Discussing confidential information with an unauthorized person;
- Failure to cooperate with the Covered Entity's Privacy Officer;
- Any unauthorized use or disclosure of PHI;
- Failure to comply with a mitigation decisions;
- Obtaining PHI under "false pretenses"; or
- Using and/or disclosing PHI for commercial advantage, personal gain or malicious harm.

TRAINING POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individual health information. Federal, state, and/or local laws and regulations have established standards with which we must comply to ensure the security and confidentiality and use and disclosure of PHI. Covered Entity also recognizes that Individual rights are a critical aspect of maintaining quality care and service, and is committed to allowing Individuals to exercise their rights under HIPAA and other applicable federal, state, and/or local laws and regulations

II. PURPOSE

The purpose of this Policy is to provide guidance to personnel as to the training requirements imposed by the Privacy Rule.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.530(b)

IV. PROCEDURE

A. General Requirement. All members of Covered Entity's workforce will be trained, as appropriate for their jobs, on Covered Entity's Policies and Procedures regarding Individuals' PHI. These Policies pertain to use and disclosure of, and access to Individual's PHI. All workforce members shall comply with the written policies and procedures included in the Privacy Program Manual, as amended from time to time, and such compliance shall be a factor considered in each employee's evaluation. In addition, Covered Entity shall apply appropriate sanctions or discipline in compliance with Covered Entity's human resources policies and procedures (and applicable collective bargaining agreements) against every provider of its workforce that fails to comply with Covered Entity's Privacy Policies and Procedures.

B. Timing. Training will occur within a reasonable period of time upon initial employment or when the new workforce member joins the Covered Entity's workforce, and thereafter on a regular basis and as necessary to reflect any changes in the Privacy Rule or changes in Covered Entity's Policies and Procedures within a reasonable period of time after the material change becomes effective.

C. Individual Rights. Workforce members shall undergo training regarding Individuals' PHI and use and disclosure of, and access to, their PHI and this training will include, where appropriate, the following:

1) allowing Individuals to file complaints concerning Covered Entity's Policies and Procedures required by HIPAA and its compliance with such Policies and Procedures;

2) allowing Individuals to receive an appropriate Accounting of disclosures of their PHI;

3) allowing Individuals to access, inspect, and/or obtain a copy of their PHI maintained in a Designated Record Set;

4) denying a request from an Individual to access, inspect, and/or obtain a copy of their PHI;

5) providing an Individual with a written statement for the reason of a denial to inspect and copy his/her PHI;

6) allowing Individuals to request confidential communications of PHI;

7) allowing Individuals to request restriction of the uses and disclosures of their PHI;

8) allowing Individuals to request an amendment or correction to their PHI that is erroneous or incomplete;

9) denying a request from an Individual to amend or correct to their PHI that is erroneous or incomplete.

D. Privacy and Confidentiality. Training regarding the privacy and confidentiality of Individual health information will include the following:

1) uses and disclosure of PHI for treatment, payment, and health care operations;

2) uses and disclosure of PHI pursuant to Individual Authorization;

3) uses and disclosure of PHI pursuant to the Individual's opportunity to agree or disagree with the use or disclosure;

4) uses and disclosure of PHI that do not require Individual Authorization, or opportunity to agree or disagree;

5) Individuals' rights concerning their PHI;

6) any other information as necessary for the respective providers of the workforce to carry out their duties and responsibilities with respect to the proper use or disclosure of PHI.

E. Use and Disclosure. Employee training regarding use and disclosure of PHI will include the following:

1) the process by which an Individual may request access to PHI;

2) the documents to be used for Individuals to request access to PHI;

3) the process by which Covered Entity may request the use or disclosure of an Individual's PHI;

4) the documents to be used for Covered Entity to solicit a request for an Individual's PHI;

5) the right of an Individual to revoke an Authorization;

6) the identification of defective Authorizations;

7) the recognition of when Covered Entity may condition the provision to an Individual of treatment, payment, enrollment, or eligibility for benefits on the provision of obtaining an Authorization.

F. Privacy Officer. Training will be conducted by the Privacy Officer or designee.

G. Execution of Employee Confidentiality Agreement. The execution of an employee confidentiality agreement is required as a condition of employment/contract/association/appointment with the Covered Entity. All Covered Entity employees and persons associated with the Covered Entity are to sign the confidentiality agreement at the commencement of their relationship with the Covered Entity if they come into contact with PHI. See Confidentiality Agreement attached hereto.

H. Documentation. All training shall be documented and retained in accordance with the Record Retention Policy.

EMPLOYEE CONFIDENTIALITY AGREEMENT

I, the undersigned, have received training on, and been afforded an opportunity to ask questions regarding, the Covered Entity's HIPAA Policies and a(n electronic) copy has been provided for me to read. I agree to ask questions on any issues that are unclear to me or that I do not understand. In consideration of my employment or association with the Covered Entity and as an integral part of the terms and conditions of my employment or association, I hereby agree that I will not at any time, during my employment or after my employment or association ends, access or use PHI, or reveal or disclose to any persons within or outside the Covered Entity, any PHI except as may be required in the course of my duties and responsibilities and in accordance with applicable local, state or federal laws governing proper release of information.

I also understand that unauthorized use or disclosure of PHI will result in disciplinary action up to and including termination of employment or association and the possible imposition of fines pursuant to applicable state and federal laws.

_____ _____

Employee signature Date

_____

Department

I have discussed the HIPAA privacy and security rules and policies and the consequences of a breach with the above named.

_____ _____

Privacy Officer or designee Date

VERIFICATION OF IDENTITY POLICY

I. POLICY

Covered Entity is committed to ensuring the privacy and security of Individuals' PHI. In the normal course of business and operations, Covered Entity will receive requests to disclose PHI for various purposes. To support our commitment to confidentiality, Covered Entity will ensure that appropriate steps are taken to verify the identity and authority of Individuals and entities requesting PHI, as required by HIPAA and other federal, state and/or local laws and regulations.

II. PURPOSE

The purpose of this policy is to provide guidance and ensure compliance with provisions of the Privacy Rule related to verifying the identity and authority of persons requesting disclosure of PHI.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.514(h)

IV. PROCEDURE

A. General Rule Regarding Use or Disclosure of PHI. In general, Covered Entity may not use or disclose PHI, without an Individual's prior Authorization, unless the use or disclosure is for treatment, payment or health care operations purposes, or otherwise expressly permitted under the Privacy Rule.

B. Exceptions to the General Rule. There are circumstances under which Covered Entity may disclose PHI, without an Authorization, in response to requests from various entities, including but not limited to public health authorities, law enforcement, courts of law and administrative tribunals. In these situations, Covered Entity must verify the identity and authority of the person or entity making the request if the identity or any such authority of such person is not known to the Covered Entity.

C. Reasonable Reliance. If the Covered Entity conditions disclosure on particular documentation for verification, the Covered Entity may rely, if such reliance is reasonable under the circumstances, on documentation that, on its face, meet the requirements. Verification may be satisfied by, for example, an administrative subpoena or a written statement that demonstrates that the requirement has been satisfied. However, the documentation must be signed and dated.

D. Procedures for Verification of Identity and Authority of Public Officials. In verifying the identity and legal authority of a public official or a person acting on behalf of the public official requesting disclosure of PHI:

1) Covered Entity personnel may rely on the following, if such reliance is reasonable under the circumstances, when disclosing PHI:

a) Documentation, statements, or representations that, on their face, meet the applicable requirements for a disclosure of PHI;
b) Presentation of an agency identification badge, other official credentials, or other proof of government status, if the request is made in person;
c) A written statement on appropriate government letterhead that the person is acting under the government's authority;
d) Other evidence or documentation from an agency, such as a contract for services, a memorandum of understanding that establishes that the person is acting on behalf of a public official;
e) A written statement of the legal authority under which the information is requested or if a written statement would be impracticable, an oral statement of such legal authority;
f) A request that is made pursuant to a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal that is presumed to constitute a legal authority.

2) Whenever possible, a copy of the applicable identification and/or evidence of legal authority should be made for retention in Covered Entity's files.

E. Covered Entity personnel may rely on the exercise of professional judgment and follow the requirements of applicable state law and other law, in consultation with legal counsel, in making the following uses or disclosures of PHI:

1) Use or disclosure to others for involvement in the Individual's care or payment for care; or

2) Disclosure to avert a serious threat to health and safety.

3) Prior to a disclosure being made under these circumstances, Covered Entity personnel should contact the Privacy Officer and/or the Legal Department.

a) Personnel will document the identity of the Individual, the authority under which he or she is requesting information, the information requested and the date of the request. This information will be forwarded, along with the request, to the Privacy Officer.
b) Once it is determined that the use or disclosure is appropriate, Covered Entity personnel with appropriate access clearance will access the Individual's PHI using proper procedures.
c) The requested PHI will be delivered in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have authorization to access that information.
d) The Privacy Officer will appropriately document the request and delivery of PHI.
e) If the identity and legal authority of an Individual or entity requesting PHI cannot be verified, employees may not disclose the requested information and will report the case to the Privacy Officer in a timely manner.

HIPAA SECURITY MANUAL

GENERAL SECURITY COMPLIANCE

The Covered Entity is committed to conducting business in compliance with all applicable laws, regulations and the Covered Entity policies. the Covered Entity has adopted this policy to set forth its compliance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the security of Electronic PHI ("EPHI")(the "Security Regulations").

This Policy covers the Covered Entity's approach to compliance with the Security Regulations. As a covered entity under the Security Regulations, the Covered Entity must:

(1) Ensure the confidentiality, integrity and availability of all EPHI the Covered Entity creates, receives, maintains or transmits;

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and

(4) Ensure compliance with the Security Regulations by its Workforce.

Compliance with the Security Regulations will require the Covered Entity to implement:

Administrative Safeguards--those actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect EPHI and to manage the conduct of the Covered Entity's Workforce in relation to the protection of and authorized access to said EPHI.

Physical Safeguards--those physical measures, policies and procedures to protect the Covered Entity's electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Technical Safeguards--the technologies and the policies and procedures for its use that protect EPHI and control access to it.

The Security Regulations permit the Covered Entity to implement any security measure that allows it to reasonably and appropriately comply with a specific security standard in the Security Regulations. In determining which security measures to implement, the Covered Entity has taken into account its size, complexity and capabilities; technical infrastructure; hardware and software security capabilities; the costs of the security measures; and the probability and criticality of potential risks to EPHI. The Covered Entity has divisions, departments or subgroups who have different uses of PHI for the Covered Entity. These groups will be referred to in this Security Manual as "Departments". In the Security Policies, the Covered Entity has determined that Departments in some cases must implement a particular security measure and in other cases have discretion to determine which security measures to implement. In those cases in which a Security Policy permits a Department to exercise discretion in the implementation of a security measure, the Department must notify and obtain the prior approval of the Security Officer for the measure implemented so that the Covered Entity may ensure that it complies with the Security Regulations.

ASSIGNED SECURITY RESPONSIBILITY POLICY

I. POLICY

On behalf of its covered entity component parts, the Covered Entity has designated a Security Officer with overall responsibility for the development and implementation of policies that conform to the Security Regulations, and to provide strategic direction and tactical management to ensure the security, confidentiality, availability, and integrity of EPHI.

The Covered Entity's HIPAA Security Officer is Russell Wood. His contact information is:

Russell Wood
russell.wood@cicsmhds.org
123 1st Ave SW, (PO Box58)
Hampton IA 50441
641-456-2128
Fax 641-456-2852

II. PURPOSE

The purpose of this policy is to establish the duties and responsibilities of the Security Officer and each of the HIPAA Security Liaisons.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.308(a)(2)

IV. PROCEDURES

1) The Security Officer and each HIPAA Security Liaison shall oversee the development, implementation and operation of Covered Entity's HIPAA Security Program. The Security Officer and/or each HIPAA Security Liaison shall have the following responsibilities:

   a) Develop and revise as needed these HIPAA Security Policies and Procedures and other mechanisms as necessary to address identified security threats and vulnerabilities to the confidentiality, integrity and availability of EPHI;
   b) Answer all questions from employees concerning the EPHI security safeguards, policies and procedures that are not adequately addressed by immediate supervision;
   c) Prepare cost benefit analyses of appropriate EPHI safeguards and make recommendations to management regarding the adoption of safeguards;
   d) Prepare the annual budgets for EPHI security;
   e) Meet with appropriate Individuals, including senior executives, the Privacy Officer and the Director of Compliance periodically, to discuss ePHI security issues, policies and planning;

f) Ensure that all ePHI security policy and procedure manuals and materials are kept up to date and current with government rules, regulations and practices;

g) Monitor Covered Entity's compliance with applicable ePHI security laws and regulations; monitor compliance with these HIPAA Security Policies and Procedures among Covered Entity employees and other third parties, and refer issues to appropriate managers or administrators;

h) Maintain records of access authorizations and document and review the levels of access granted to a user, program, or procedure accessing ePHI on an ongoing basis;

i) Develop appropriate ePHI security training program for Covered Entity employees;

j) Prepare and periodically assess Covered Entity's security incident response procedures, disaster recovery plan and business continuity plan for information systems containing ePHI;

k) Perform security audits and risk assessments of ongoing system activities utilizing ePHI;

l) Provide consulting support and make recommendations to management regarding appropriate, timely and necessary improvements or enhancements to the ePHI security program;

m) Coordinate ongoing review of existing ePHI security programs and initiate the development of new programs, as needed;

n) Investigate ePHI system security breaches, and, in consultation with the Privacy Officer (or designees), and administer appropriate sanctions related to security violations; and

o) Facilitate a process for Individuals to file a complaint regarding the Covered Entity's Security Policies or the handling of EPHI by a Covered Entity HIPAA health care component., including ensuring that the complaint and its disposition are appropriately documented and handled.

2) HIPAA Security Liaisons. The t HIPAA Security Liaison is responsible for assisting the HIPAA Security Officer in ensuring that the Department:

a) Complies with the HIPAA Security Policies

b) Develops and implements department specific HIPAA Security Procedures for each Security Policy that is applicable to that department,

c) Maintains the confidentiality of all EPHI created or received by the department from the date such information is created or received until it is destroyed, and

d) Trains all Workforce members within the Department at the appropriate level of HIPAA training as determined by the HIPAA Security Officer.

RISK ANALYSIS POLICY

I. POLICY

The Covered Entity acknowledges the potential vulnerabilities associated with storing EPHI, transmitting EPHI locally, transmitting EPHI outside of the Covered Entity, and transmitting EPHI to the Covered Entity components that are not health care component parts. The Covered Enmity will identify and assess the system's vulnerabilities and any threats to the confidentiality, integrity, and availability of the ePHI on a periodic basis.

II. PURPOSE

The purpose of this policy is to establish guidelines for the periodic and accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of the EPHI Covered Entity maintains.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.308(a)(1)(ii)(A)

IV. PROCEDURES

1) The Security Officer and each HIPAA Security Liaison shall:

   a) Identify and document all EPHI repositories, including present security controls or features in each repository
   b) Periodically re-inventory EPHI repositories
   c) Identify the potential vulnerabilities to each EPHI repository,
   d) Assess the probability that the vulnerability would be exploited;
   e) Assign a level of risk to each EPHI repository
   f) Determine risk mitigation strategies and appropriate mechanisms, safeguards, and controls
   g) Document the process; and
   h) Document the results.

2) All repositories of EPHI will be identified and logged into a common catalogue. An EPHI repository may be in the form of a database, spreadsheet, folder, storage device, document or other form of electronic information that is accessed by one or more users. Each repository will be logged with the appropriate level of file, system, and owner information including, but not limited to:

   a) Repository Name
   b) Custodian Name
   c) Custodian Contact Information
   d) Number of Users that access the repository
   e) Number of Records
   f) System Name
   g) System Location
   h) System Manager Contact Information

i) Risk Level

3) The Security Officer and each HIPAA Security Liaison shall update EPHI inventory for each Department as needed to ensure that the EPHI catalogue is up to date and accurate. Each identified EPHI repository will be analyzed for any potential vulnerability to the integrity, confidentiality, and availability of its EPHI. The following two-dimensional model will be used to assign a risk level to each EPHI repository.

   a) High Risk – Repositories with a large number of records accessed by a large numbers of users
   b) Medium Risk – Repositories with either a large number of records and a small number of users or a small number of records and a large number of users
   c) Low Risk – Repositories with a small number of records accessed by a small number of users

4) Each HIPAA Security Liaison shall assist the Security Officer in reassessing the potential risks and vulnerabilities to the integrity, confidentiality, and availability of each EPHI repository and the level of risk assigned to each EPHI repository as needed.

5) EPHI repositories that otherwise would fall in the low or medium risk categories may be classified as high risk EPHI if the sensitivity or criticality of that information makes it appropriate to do so in the reasonable judgment of the HIPAA Security Liaison and the HIPAA Security Officer.

RISK MANAGEMENT POLICY

I. POLICY

The Covered Entity will select and implement appropriate, cost-effective safeguards and will institute corrective action as necessary to protect the confidentiality, integrity, and availability of EPHI.

II. PURPOSE

The purpose of this policy is to ensure that Covered Entity implements security measures that are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. § 164.308(a)(1)(ii)(B)

IV. PROCEDURES

1) The level, complexity and cost of such security measures and safeguards shall be commensurate with the risk classification of each such EPHI repository. The diverse nature of the Departments within the Covered Entity's HIPAA health components necessitates a high level of autonomy in planning, designing and implementing HIPAA security measures and safeguards. Each Department must meet the following minimum guidelines in implementing security measures and safeguards:

    a) Low risk EPHI repositories may be appropriately safeguarded by normal best-practice security measures in place such as user accounts, passwords and perimeter firewalls.
    b) Medium and high risk EPHI repositories must be secured in accordance with HIPAA Security Policies and Procedures.

2) Covered Entity will evaluate the following factors when selecting and implementing administrative, physical and technical security safeguards:

    a) The size, complexity, and capabilities of Covered Entity;
    b) Covered Entity's technical infrastructure, hardware, and software security capabilities;
    c) The costs of the security measures;
    d) The probability and criticality of potential risks to ePHI;
    e) The feasibility of implementation and use (e.g., compatibility, user acceptance); and
    f) The effectiveness (e.g., degree of protection and level of risk mitigation) of the mechanism, process or safeguard.

3) Covered Entity will assign appropriate Workforce members or external staff who possess the requisite expertise and skill sets to implement the selected security safeguards.

4) To the extent possible, Covered Entity will schedule the implementation of appropriate security safeguards without undue disruption to business operations.

5) To the extent the Security Officer and a HIPAA Security Liaison reassesses the potential risks and vulnerabilities of an EPHI repository as part of a periodic review; the Security Officer shall update the security measures and safeguards for such EPHI repository to reflect any changes in the risks and vulnerabilities assessment.

SANCTION POLICY

I. POLICY

The Covered Entity shall enforce appropriate discipline and sanction employees and other Workforce members for any violation of Security Policies and Procedures.

II. PURPOSE

The purpose of this policy is to notify Workforce members that Covered Entity will undertake disciplinary action against any Workforce member who violates these HIPAA Security Policies and Procedures.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(1)(ii)(C)
- Sanction Policy (Privacy Policies)

IV. PROCEDURES

1) To ensure that all users of Covered Entity's systems fully comply with these HIPAA Security Policies and Procedures, Covered Entity, will discipline and sanction such users, as appropriate, for any violation of the HIPAA Security Policies and Procedures.

2) Sanctions will be applied according to the Covered Entity's Sanction Policy as set forth in the Covered Entity's Privacy Policy, attached hereto and incorporated herein.

INFORMATION SYSTEM ACTIVITY REVIEW POLICY

I. POLICY

The Covered Entity will collect and review data generated by system activity and will implement additional security safeguards or corrective action when necessary.

II. PURPOSE

The purpose of this policy is to monitor system activity through the periodic review of activity and records including audit logs, access reports, and security incident tracker reports.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(1)(ii)(D)
- Risk Management Policy
- Incident Procedures Policy

IV. PROCEDURES

1) To ensure that system activity for all systems classified as medium and high risk is appropriately monitored and reviewed, the Security Officer and each HIPAA Security Liaison shall follow the minimum procedures outlined below:

   a) An internal audit procedure has been established and implemented by each HIPAA Security Liaison and the Security Officer to regularly review records of system activity. The internal audit procedure utilizes audit logs, activity reports, and other mechanisms to document and manage system activity.

   b) Audit logs, activity reports, and other mechanisms to document and manage system activity are reviewed at intervals commensurate with the associated risk of the information system or the EPHI repositories contained on said information system.

   c) An Audit Control and Review Plan has been created by the Security Officer and each HIPAA Security Liaison and has been approved by the HIPAA Security Officer. These plans include:

      i. Systems and Applications to be logged
      ii. Information to be logged for each system
      iii. Procedures to review all audit logs and activity reports

   d) At a minimum, Covered Entity will review login IDs, dates, times, and session times so as to identify:

      i. unauthorized access and/or attempts to access to ePHI
      ii. unauthorized modification of, and attempts to modify ePHI
      iii. attempts to exceed access authority
      iv. attempts to gain system access during unusual hours

v. unusual levels of activity that are inconsistent with a workforce member's job functions; and

vi. sustained activity levels for extended periods of time, inconsistent with a workforce member's scheduled work hours.

e) Security incidents such as activity exceptions and unauthorized access attempts if they occur will be detected, logged and reported immediately to the appropriate HIPAA Security Liaison and the Security Officer in accordance with the HIPAA Security Incident Response and Reporting Policy.

f) The Covered Entity will undertake corrective action and will implement additional security safeguards as appropriate and consistent with the Risk Management Policy and Security Incident Procedures Policy.

AUTHORIZATION AND/OR SUPERVISION POLICY

I. POLICY

Covered Entity will authorize Covered Entity employees whose job function requires the use of EPHI to have access to EPHI.

II. PURPOSE

The purpose of this policy is to ensure that appropriate Individuals are authorized to have access to ePHI.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(3)(ii)(A)
- Workforce Clearance Policy
- Access Control and Validation Procedures Policy

IV. PROCEDURES

1) Covered Entity will authorize access to EPHI to those employees who require such access in order to perform his or her job.

   a) Covered Entity will review such access authorizations as appropriate.
   b) Access authorizations shall be revoked upon termination of employment or when access to EPHI is no longer necessary.

2) Whenever Covered Entity engages another person or entity (other than an officer, director or employee of Covered Entity) to perform or assist in the performance of Covered Entity business functions that will result in that person or entity creating, receiving, maintaining or transmitting EPHI on behalf of Covered Entity, Covered Entity must enter into a Business Associate Agreement with such party.

3) Covered Entity will maintain a list of those employees who require access to and are authorized to access ePHI. The Individuals who are entitled to access EPHI are listed in the Security Officer's files or in the files of each covered office.

HIPAA WORKFORCE CLEARANCE POLICY

I. POLICY

The Security Officer, the Privacy Officer or the Director of Human Relations (or their designees) will screen all members of the Workforce and other Individuals prior to granting access to EPHI.

II. PURPOSE

The purpose of this policy is to ensure that all members of the workforce have been properly cleared to gain access to EPHI and the appropriate level of access to EPHI is granted.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(3)(i)(B)
- Information Access Management Policy

IV. PROCEDURES

1) A background check must be performed by the Department Head on all workforce members requiring access to EPHI repositories. The background check must be completed and deemed satisfactory by the Security Officer and each HIPAA Security Liaison before access to high risk EPHI is granted.

2) All employees must complete the security training program, within two months of hire, in order to obtain authorization and access rights to ePHI.

3) Each Department must comply with the policies and procedures for authorizing, managing, and terminating access to EPHI for workforce members detailed in HIPAA Security Information Access Management Policy.

4) All the Covered Entity workforce members are subject to the attached Covered Entity Code of Conduct as it relates to the appropriate use of PHI and EPHI.

ATTACHMENT TO WORKFORCE CLEARANCE POLICY

Covered Entity Code of Conduct

This code applies to:

1) Individuals who are paid by the Covered Entity when they are working for the Covered Entity;

2) Consultants, vendors, and contractors when they are doing business with the Covered Entity; and

3) Individuals who perform services for the Covered Entity as volunteers.

The Code of Conduct refers to all these persons collectively as "members of the Covered Entity community" or "community members."

Integrity and Ethical Conduct the Covered Entity is committed to the highest ethical and professional standards of conduct as an integral part of its mission. To achieve this goal, the Covered Entity relies on each community member's ethical behavior, honesty, integrity, and good judgment. Each community member should demonstrate respect for the rights of others. Each community member is accountable for his or her actions. This Code of Conduct describes standards to guide us in our daily Covered Entity activities.

Compliance with Laws and Covered Entity Policies the Covered Entity and each community member must transact Covered Entity business in compliance with all laws, regulations, and Covered Entity policies related to their positions and areas of responsibility. Department Heads are responsible for teaching and monitoring compliance in their departments.

Procedures for Reporting Violations or Concerns the Covered Entity's compliance effort focuses mainly on teaching members of the Covered Entity community the appropriate compliance standards for the areas in which they work. Nevertheless, violations may occur. In addition, members of the Covered Entity community may have concerns about matters that they are not sure represent violations. Each community member is expected to report violations or concerns about violations of this Code of Conduct that come to his/her attention. Department Heads have a special duty to adhere to the standards set forth in this Code of Conduct, to recognize violations, and to enforce the standards. Disciplinary actions for proven violations of this Code, or for retaliation against anyone who reports possible violations, will be determined on a case by- case basis and may include termination of employment. Individuals who violate the Code may also be subject to civil and criminal charges in some circumstances.

How to Report a Violation or Discuss a Concern You may report violations or concerns to your immediate supervisor or department head, if appropriate. You may also call the **HIPAA Compliance Office at the number established for this purpose: [641-456-2128]**. Reports may be made anonymously to this number, if the caller so desires.

TERMINATION PROCEDURES POLICY

I. POLICY

Covered Entity shall terminate authorization and access rights of employees to EPHI upon termination of employment or when such access to EPHI is no longer necessary.

II. PURPOSE

The purpose of this policy is to terminate EPHI access and authorization rights for those Individuals who no longer have a need to access Covered Entity's EPHI.

III. REFERENCES/CROSS-REFERENCES

- 45 C.F.R. §164.308(a)(3)(ii)(C)
- Authorization and/or Supervision Policy
- Information Access Management Policy

IV. PROCEDURES

1) If a workforce member's employment is terminated or a workforce member leaves the Covered Entity, the workforce member's supervisor or manager must ensure that all accounts to access EPHI are terminated.

2) The workforce member's supervisor or manager must ensure that access to all facilities housing EPHI has been terminated. This includes, but is not limited to, card access, keys, codes, and other facility access control mechanisms. Codes for key punch systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate.

3) The HIPAA Security Liaison and the Security Officer should be notified and the termination processed in accordance with the termination checklist attached to this policy.

4) If a workforce member transfers to another department or workgroup, the workforce member's existing supervisor or manager must ensure that all accounts to access EPHI are terminated. The Workforce member's new supervisor or manager is responsible for requesting access to EPHI commensurate with the workforce member's new role.

5) Under no circumstances will access to EPHI be extended to workforce members beyond the final date of their employment unless a Business Associates Arrangement or Contract is filed in accordance to the Covered Entity Privacy Policies.

ATTACHMENT TO TERMINATION PROCEDURES POLICY

TERMINATION CHECK LIST

Employee Name: _____ Department: _____
Actual Last Day Worked: _____ Division: _____

Upon notification of an employee's termination, the Department Head should be contacted immediately by the employee's supervisor. The following items (if applicable) must be collected by the employee's immediate supervisor and sent to the appropriate Individual for processing.

[ ] Letter of resignation/Letter of Termination

[ ] Forwarding address obtained

[ ] Final time sheet/accounting of hours worked

[ ] Final performance evaluation completed
[ ] Vacation to be taken prior to actual last day worked: _____
[ ] Final check disposition obtained
[ ] Direct deposit to be cancelled for last check: _____Yes _____No
[ ] the Covered Entity parking permit including any corporate Handicap Parking Permits

[ ] the Covered Entity I.D. card enclosed

[ ] Covered Entity keys numbered: _____ enclosed
[ ] Tools/Equipment (compare to equipment disbursement list)
[ ] Other Covered Entity Property
[ ] Long Distance Card

[ ] Pagers and/or Cell Phones

[ ] Collection of personal belongings

COMPUTER SECTION

[ ] User Name Account Disabled [ ] Remote Access Disabled [ ] Hardware/devices secured

[ ] Email Disabled [ ] Loaner hardware, software, training material turned in

[ ] Other_____
Notes: _____

Forwarding Address:
Street Address: _____
City/State/Zip: _____
Phone Number: (___) _____

Signature of Immediate Supervisor indicating receipt of above information:

_____
Immediate Supervisor Signature

I acknowledge that I am no longer to access any information or accounts nor will I utilize any information that I already know in violation of HIPAA.

_____
Signature of former employee

INFORMATION ACCESS MANAGEMENT POLICY

I. POLICY

The Covered Entity will assign each workforce member a level of access based on the Individual's need for EPHI to perform his or her job function, and will document, review, and modify as appropriate the access rights of those Individuals who have been authorized to access EPHI.

II. PURPOSE

The purpose of this policy is to ensure that access to EPHI is assigned and managed in a manner commensurate with the role of each workforce member and that access to EPHI is consistent with the HIPAA Privacy Rules.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.502(b) (Minimum Necessary Policy)
- 45 C.F.R. §164.308(a)(4)(ii)(B)
- 45 C.F.R. §164.308(a)(4)(ii)(C)
- Authorization and/or Supervision Policy
- Access Establishment and Modification Policy

IV. PROCEDURES

1) The Security Officer and each HIPAA Security Liaison must implement procedures to establish, document, review and modify each workforce member's right to access EPHI. These procedures include the following responsibilities:

   a) It is the responsibility of each supervisor or manager to authorize access to systems and networks containing EPHI for each of their subordinates. Workforce members are not permitted to authorize their own access to EPHI or be granted authorization from another supervisor.
   b) It is the responsibility of each supervisor or manager to ensure that the access granted for each of their subordinates to EPHI meets the minimum requirements for their roles.
   c) It is the responsibility of each supervisor or manager to review the access granted to EPHI for each of their subordinates, adjusting their access rights as their roles change.

2) The Security Officer and/or each HIPAA Security Liaison, at his or her own discretion, may conduct further background checks into an employee's past before allowing an employee access to ePHI, including but not limited to credit history checks, criminal record checks and employment history verification

3) The Security Officer and/or each HIPAA Security Liaison may modify a workforce member's access to EPHI in his or her discretion.

4) The Security Officer and/or each HIPAA Security Liaison will maintain an inventory of users authorized to access EPHI.

5) The Security Officer and/or each HIPAA Security Liaison will document any changes to a user or workforce member's access rights on the inventory of users.

SECURITY TRAINING POLICY

I. POLICY

All workforce members who are authorized to access EPHI are required to participate in the basic and ongoing security training.

Covered Entity will issue security reminders to workforce members on a periodic basis to promote awareness of security concerns and risks.

Covered Entity will implement and update controls to guard against, detect and report malicious code. Covered Entity will ensure that all system users know the dangers of, and how to respond to, viruses, worms, and other uninvited computer code that could destroy or alter system resources, including ePHI.

II. PURPOSE

The purpose of this policy is to (i) ensure that the Covered Entity workforce is properly trained and made aware of security policies, procedures, potentials threats, and incidents; (ii) inform workforce members of security concerns on an ongoing basis; and (iii) ensure that all the Covered Entity workforce members are appropriately made aware of the threats and vulnerabilities due to malicious code and software such as viruses and worms and are appropriately trained to identify and prevent these types of attacks.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(5)
- 45 C.F.R. §164.308(a)(5)(ii)(A)
- 45 C.F.R. §164.308(a)(5)(ii)(B)

IV. PROCEDURES

1) **HIPAA Security Training**.

a) All the Covered Entity workforce members (including employees, volunteers, and trainees) that access, receive, transmit, or otherwise use EPHI or setup, manage, or maintain systems and workstations that access, receive, transmit, or store EPHI are subject to HIPAA Security Training.

b) To ensure that all the Covered Entity workforce members are appropriately made aware of all HIPAA Security Policies and Procedures and their responsibilities in relation to understanding and complying with the HIPAA Security Policies and Procedures, the following training procedures must be established and implemented:

i. The Security Officer and each HIPAA Security Liaison is responsible for ensuring that its workforce has the appropriate level of HIPAA Privacy training.

ii. The Security Officer and each HIPAA Security Liaison is responsible for ensuring that its workforce has the appropriate level

of HIPAA Security Training. The minimum level of HIPAA Security training must consist of, but is not limited to, the following requirements:

1) HIPAA Security Policies
2) HIPAA Sanction Policy
3) Confidentiality, Integrity, and Availability (CIA)
4) Individual security responsibilities
5) Common security threats and vulnerabilities

iii. The Security Officer and each HIPAA Security Liaison is also responsible for ensuring that all IT (Information Technology) staff members and all workforce members that are responsible for the setup, installation, or management of computer systems and networks containing EPHI have the appropriate level of HIPAA Security training. HIPAA Security training for these workforce members must consist of, but is not limited to, the following requirements:

1) HIPAA Security Policies
2) HIPAA Sanction Policy
3) Confidentiality, Integrity, and Availability (CIA)
4) Individual security responsibilities
5) Common security threats and vulnerabilities
6) Password Structure and Management procedures
7) Server, desktop computer, and mobile computer system security procedures including

    a. Security patch and update procedures
    b. Virus and Malicious Code protection procedures
    c. Device and Media Control procedures
    d. Incident response and reporting procedures (See HIPAA Security Incident Response and Reporting Policy)

iv. The Security Officer and each HIPAA Security Liaison must also ensure that the appropriate IT staff is aware of and trained to comply with the following HIPAA Security policies and procedures:

1) Login Monitoring procedures (See HIPAA Security Training and Awareness Policy)
2) Audit Control and Review Plan (See HIPAA Security Audit Control Policy)
3) Data Backup Plan (See HIPAA Security Contingency Planning Policy)
4) Disaster Recovery Plan (See HIPAA Security Contingency Planning Policy)

v. Each Department must maintain formal documentation of the current level of HIPAA training for each of its workforce members.

2) **Security Reminders**.

a) The Security Officer and each HIPAA Security Liaison is responsible for ensuring that its workforce is made aware of all changes or updates to HIPAA Security policies and procedures.

b) The Security Officer and each HIPAA Security Liaison must establish and implement a procedure to disseminate security reminders to its workforce to make them aware of any of the following events:

i. A new HIPAA Security Policy or Procedure has been approved.
ii. A current HIPAA Security Policy or Procedure has been updated.
iii. A new threat, breach or vulnerability has been discovered or reported that may affect EPHI. (See HIPAA Security Incident Response and Reporting Policy)

c) The HIPAA Security office shall notify the HIPAA Security Liaisons of any of the following events:

i. A new HIPAA Security Policy or Procedure has been approved.
ii. A current HIPAA Security Policy or Procedure has been updated.

3) **Protection from Malicious Software**

a) The Security Officer and each HIPAA Security Liaison is responsible for ensuring that its workforce is appropriately trained to identify and protect against malicious code and software.

b) The Security Officer and each HIPAA Security Liaison shall disseminate security reminders to its workforce to make them aware of any of new virus, worm, or other type of malicious code that may be a threat to EPHI.

c) Each HIPAA Security Liaison shall notify the HIPAA Security Office in the event that a virus, worm, or other malicious code has compromised or potentially compromised EPHI. (See HIPAA Security Incident Response and Reporting Policy)

d) The Security Officer [and each HIPAA Security Liaison] must notify the Covered Entity IT Department in the event that a virus, worm, or other malicious code has been identified and is a potential threat to other systems or networks. (See HIPAA Security Incident Response and Reporting Policy)

e) In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation, that system must be disconnected from the network until the system has been appropriately cleaned.

f) A virus detection system must be implemented on all workstations including a procedure to ensure that the virus detection software is maintained and up-to-date. (See HIPAA Security Server, Desktop, and Wireless Computer System Security Policy)

LOG-IN MONITORING POLICY

I. POLICY

The Security and/or System Administrators will monitor log-in attempts by unauthorized users and take corrective action as necessary.

II. PURPOSE

The purpose of this policy is to establish guidelines for the ongoing review and reporting of attempts at system access.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(5)(ii)(C)

IV. PROCEDURES

1) The Security and/or System Administrator will monitor log-ins and other attempts at system access.

2) All system users are required to report the Help Desk, or the Security Officer or appropriate designee, any suspicious log-in activity, log-in attempts, or other discrepancies.

PASSWORD MANAGEMENT POLICY

I. POLICY

The Covered Entity will ensure that all user passwords that may be used to access any system or application, or to access, transmit or store EPHI are properly safeguarded.

II. PURPOSE

The purpose of this policy is to ensure that passwords created and used by the Covered Entity workforce to access any network, system, or application used to access, transmit, receive, or store EPHI are properly safeguarded and to ensure that the workforce is made aware of all password related policies.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(a)(5)(ii)(D)

IV. PROCEDURES

1) **Password Management**

a) All workforce members that access networks, systems, or applications used to access, transmit, receive, or store EPHI must be supplied with a Unique User Identification and password to access the aforementioned EPHI. (See HIPAA Security Unique User Identification Policy)

b) All workforce members must supply a password in conjunction with their Unique User Identification to gain access to any application or database system used to create, transmit, receive, or store EPHI. (See HIPAA Security Unique User Identification Policy)

c) A generic User Identification and Password may be utilized for access to shared or common area workstations so long as the login provides no access to EPHI. An additional Unique User Identification and Password must be supplied to access applications and database systems containing EPHI.

d) All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store EPHI must be of sufficient complexity to ensure that it is not easily guessable. (See HIPAA Security Password Structure Policy)

e) Managers of networks, systems, or applications used to access, transmit, receive, or store EPHI, must ensure that passwords set by workforce members meet the minimum level of complexity as defined in HIPAA Security Password Structure Policy.

f) Password aging times shall be implemented in a manner commensurate with the criticality and sensitivity of the EPHI contained within each network, system, application or database but shall not be longer than 90 days.

g) Workforce members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:

i. Passwords are only to be used for legitimate access to networks, systems, or applications.
ii. Passwords must not be disclosed to other workforce members or Individuals.
iii. Workforce members must not allow other workforce members or Individuals to use their password.
iv. Passwords must not be written down, posted, or exposed in an unsecured manner such as on a notepad or posted on the workstation or under the keyboard.

h) If a workforce member knows that the confidentiality of his or her password has been compromised, he or she must contact the Security Officer or HIPAA Security Liaison immediately. The [System Administrator] will enable the workforce member to set a new and different password.

2) **Password Structure**. To ensure that all passwords used to control access to any network, system, application, media or file containing EPHI are secure and not easily guessed, the following procedures must be followed:

a) Passwords must be a minimum of eight characters in length.
b) Passwords must incorporate at least three of the following characteristics:

i. Any lower case letters (a-z)
ii. Any upper case letters (A-Z)
iii. Any numbers (0-9)
iv. Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ `)

c) Passwords must not include easily guessed information such as personal information, names, pets, birthdates, etc.
d) Passwords must not be words found in a Dictionary.
e) If a system does not support the minimum structure and complexity as detailed in the aforementioned guidelines, the password assigned must be adequately complex to ensure that it is not easily guessed.
f) If an alternative password structure must be implemented, the complexity of the chosen alternative must be defined and documented, and then:

i. The legacy system must be upgraded to support the minimum HIPAA Security Password Structure, or
ii. All EPHI must be removed and relocated to a system that supports the minimum HIPAA Security Password Structure.

g) All passwords shall have longevity not to exceed 90 days.

INCIDENT PROCEDURES POLICY

I. POLICY

The Covered Entity will implement procedures for responding to and reporting suspected or known security incidents.

II. PURPOSE

The purpose of this policy is to ensure that all HIPAA security incidents and violations are appropriately identified, reported, mitigated and documented.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(6)(ii)

IV. PROCEDURES

1) A common HIPAA Incident Response and Reporting System has been setup and implemented to support the reporting, mitigation, and documentation of HIPAA security and privacy incidents and violations.

2) All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of EPHI must be reported using the following procedures:

   a) Users must notify the Appropriate IT personnel for issues involving viruses, local attacks, Denial of Service (DOS) attacks, etc. the reporting processes should include the following steps:

      i. Notify Appropriate IT personnel

         1) The Appropriate IT personnel investigates and propagates updates or fixes.
         2) The Appropriate IT personnel notifies the HIPAA Security Officer if threat to EPHI.
         3) Notify security liaison if incident may involve EPHI
         4) If the security liaison is unavailable, notify the HIPAA Security Officer

      ii. It is the responsibility of each security liaison to aggregate and assess the severity of incidents within their Departments involving EPHI and report those incidents, when appropriate, to the HIPAA Security Officer.

3) Incidents that should be reported include, but are not limited to:

   a) Virus, worm, or other malicious code attacks
   b) Network or system intrusions
   c) Persistent intrusion attempts from a particular entity

d) Unauthorized access to EPHI, EPHI based system, or EPHI based network
e) EPHI data loss due to disaster, failure, error

4) The HIPAA Security Officer shall notify the Appropriate IT personnel if a security incident involves an outside entity or traverses the network.

5) The Appropriate IT personnel must notify the HIPAA Security Officer if they are notified of or detect an incident they feel may impact EPHI systems or data.

6) All HIPAA related incidents, security and privacy, must be logged and documented by each Department. The HIPAA Security and Privacy Officer will also be responsible for documenting and logging incidents related to HIPAA Privacy and Security. The HIPAA Security Officer must notify the HIPAA Security Liaisons of Policy Updates and Changes, Virus or other malicious software updates, Covered Entity-wide threats to EPHI, etc. HIPAA Security Liaisons must propagate recommendations, policy and procedures changes, and security reminders to their Departments.

7) Disaster Recovery reporting procedures must include the following:

a) All instances of failures, outages, or data loss that involve critical EPHI must be logged internally within the Department (See HIPAA Security Contingency Planning Policy).
b) All instances of failures, outages, or data loss that involve critical EPHI must be reported to the HIPAA Security Officer.
c) All correspondence with outside authorities such as local police, FBI, media, etc. must go through the Covered Entity Attorney, HIPAA Security Liaison and the Security Officer.

BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS POLICY

I. POLICY

All agreements with business associates that create, receive, maintain, or transmit ePHI on behalf of Covered Entity must include security related provisions that comply with the Security Rules and HITECH.

II. PURPOSE

The purpose of this policy is to protect, through the execution and enforcement of written agreements, the privacy and confidentiality of ePHI created, received, maintained or transmitted by Covered Entity's business associates its behalf.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164. 164.308(b)
- 45 C.F.R. §164.504(e)
- Emergency Mode Operation Plan Policy
- HIPAA Privacy Policies and Procedures: Business Associate Policy

IV. PROCEDURES

1) Covered Entity will identify those business associates that create, receive, maintain, or transmit ePHI and will enter into a business associate agreement with such business associate that includes:

   a) language that requires the business associate to comply with the Security Rule's administrative, technical and physical safeguards and policies and procedure requirements in the same manner as the requirements apply to the plan;
   b) provisions that ensure that any agent, including a subcontractor, to whom the business associate provides the ePHI agrees to implement reasonable and appropriate safeguards;
   c) provisions that require the business associate to report to Covered Entity certain security incidents of which the business associate becomes aware;
   d) provisions that authorize termination of the contract by Covered Entity if Covered Entity determines that the business associate has violated a material term of the contract.

2) To ensure that access to critical EPHI is maintained during an emergency situation, the following emergency access measures must be implemented:

   a) If a system contains EPHI used to provide medical services, and the denial or strict access to that EPHI could inhibit or negatively affect Individual care, the Departmental HIPAA Security Liaison and the Security Officer have implemented procedures to ensure that access to that system is made available to any caregiver in case of an emergency in accordance with state and federal law.

b) This policy applies to all EPHI repositories that affect Individual care. Many repositories are not used for Individual care, and do not fall under this policy.

ADMINISTRATIVE SAFEGUARDS CONTINGENCY PLAN POLICY

I. POLICY

Covered Entity will develop procedures to permit access to its systems containing ePHI to Individuals who are responding to an emergency or catastrophic failure of any system, application or data, while preventing access to unauthorized personnel.

II. PURPOSE

The purpose of this policy is to establish procedures regarding facility access (i) in support of data restoration activities under the disaster recovery plan, or (ii) in the event of an emergency under the emergency mode operations plan.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(a)(ii)(A)
- Disaster Recovery Plan Policy
- Emergency Mode Operation Plan Policy
- Authorization and/or Supervision Policy

IV. PROCEDURES

These procedures are covered in the Risk Analysis, Emergency Mode Operations, and Data Disaster Recovery Plan for each covered department, which is attached.

DATA BACKUP PLAN POLICY

I. POLICY

The purpose of this policy is to ensure that EPHI will not be irretrievably destroyed or lost in the event of an emergency or other occurrence.

II. PURPOSE

It is Covered Entity's policy to have access to retrievable, exact copies of EPHI.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)(ii)(A)
- 45 C.F.R. §164.310 (d)(2)(iv)
- Integrity and Authentication Policy

IV. PROCEDURES

1) **Data Backup Plan**

   a) The Security Officer and each HIPAA Security Liaison has established and implemented a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all EPHI determined to be medium and high risk.

   b) The Data Backup Plan applies to all medium and high risk files, records, images, voice or video files that may contain EPHI.

   c) The Data Backup Plan requires that all media used for backing up EPHI be stored in a physically secure environment, including a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.

   d) The Data Backup Plan factors in the cost of the backup and the likelihood of inability to function in the event that the data was lost.

   e) The Security Officer will determine which information must be retrievable for Covered Entity to continue to function as usual in the event of damage or destruction of the data, hardware, or software.

   f) Data backup procedures outlined in the Data Backup Plan must be tested on a periodic basis to ensure that exact copies of EPHI can be retrieved and made available.

   g) Each HIPAA Security Liaison with medium and high risk EPHI has submitted its Data Backup Plan to the HIPAA Security Officer for approval.

2) **Off-Site Storage Facility or Backup Service**. When an off-site storage facility or backup service is used, a written contract or Business Associate Agreement is used to ensure that the Business Associate will safeguard the EPHI in an appropriate manner.

DISASTER RECOVERY PLAN POLICY

I. POLICY

The purpose of this policy is to ensure that, in the event of an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing EPHI, Covered Entity can restore or recover any loss of EPHI and the systems needed to make that EPHI available in a timely manner.

II. PURPOSE

It is Covered Entity's policy to have access to backed-up and stored data and to recover any lost data in the event of a disaster or system failure.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)(ii)(B)
- 45 C.F.R. §164.312 (a)(2)(ii)

IV. PROCEDURES

1) **Responsibility for Disaster Recovery Plan**. The Security Officer [and each HIPAA Security Liaison] shall be responsible for establishing and implementing the Disaster Recovery Plan.

2) **Disaster Recovery Plan Requirements**

a) The Disaster Recovery Plan includes procedures to restore EPHI from data backups in the case of a disaster causing data loss.

b) The Disaster Recovery Plan includes procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

c) The Disaster Recovery Plan, at a minimum, contains the following requirements:

i. Covered Entity will conduct a daily backup
ii. The daily backup will only backup changes from the previous day
iii. Each Friday, a full system backup shall be conducted
iv. The daily backup tape will be kept onsite, but in a different, physically secure room from other servers
v. The weekly backup shall be kept at any offsite, secure location designed specifically for the purpose of storing backup data.

d) The Disaster Recovery Plan is documented and easily available to the necessary personnel at all times, who are trained to implement the Disaster Recovery Plan .

e) The disaster recovery procedures outlined in the Disaster Recovery Plan are tested on a periodic basis to ensure that EPHI and the systems needed to make EPHI available can be restored or recovered.

3) **Approval**. Each HIPAA Security Liaison with medium and high risk EPHI has submitted its Disaster Recovery Plan to the HIPAA Security Officer for approval.

V. These procedures are covered in the Risk Analysis, Emergency Mode Operations, and Data Disaster Recovery Plan for each covered department, which is attached.

EMERGENCY MODE OPERATION PLAN POLICY

I. POLICY

The purpose of this policy is to enable continuation of critical business processes for protection of the security of EPHI after the occurrence of a disaster or other event that triggered the necessity to operate in emergency mode.

II. PURPOSE

Covered Entity will establish and maintain procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)(ii)(C)

IV. PROCEDURES

1) The Security Officer and each HIPAA Security Liaison shall establish and implement (as needed) emergency mode operation procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.

2) Emergency mode operation procedures outlined in the Emergency Mode Operation Plan shall be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

3) Each HIPAA Security Liaison with medium and high risk EPHI must submit its Emergency Mode Operation Plan to the HIPAA Security Officer for approval.

These procedures are covered in the Risk Analysis, Emergency Mode Operations, and Data Disaster Recovery Plan for each covered department, which is attached.

APPLICATIONS AND DATA CRITICALITY ANALYSIS

I. POLICY

Covered Entity will assess the relative criticality of specific software applications and data in support of other contingency plan components.

II. PURPOSE

The purpose of this policy is to provide for the security of software applications and any ePHI that is received by, stored on and/or transmitted to/from those applications.

III. REFERENCES/ CROSS REFERENCES

- 45 C.F.R. §164.308(a)(7)(ii)(E)

IV. PROCEDURES

1) The Security Officer shall assess the relative criticality of specific software applications and data in support of other contingency plan components to ensure that critical software is accessible. Such a plan shall consider:

   a) The physical and technical security of data and EPHI
   b) Access to data and critical networks, software and hardware in the event of emergency;
   c) Critical business functions.

These procedures are covered in the Risk Analysis, Emergency Mode Operations, and Data Disaster Recovery Plan for each covered department, which is attached.

PERIODIC EVALUATION POLICY

I. POLICY

The Covered Entity will conduct periodic evaluations to ensure that the safeguards chosen reasonably safeguard EPHI and otherwise satisfy the requirements of the Security Regulations.

II. PURPOSE

The purpose of this policy is to ensure that each Security Policy adopted by the Covered Entity and each Security Procedure developed and implemented by a HIPAA Security Liaison and the Security Officer is periodically evaluated for technical and non-technical viability.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.308(a)(8)

IV. PROCEDURES

1) **Periodic Evaluation Generally**. The Covered Entity Security Policies and Department Security Procedures initially should be evaluated to determine their compliance with the Security Regulations. Once compliance with the Security Regulations is established, the Covered Entity Security Policies and Department Security Procedures should be evaluated on a periodic basis to assure continued viability in light of technological, environmental or operational changes that could affect the security of EPHI.

2) **Periodic Evaluation by the Covered Entity HIPAA Security Officer**

   a) The HIPAA Security Officer will review on an on-going basis the viability of the Covered Entity Security Policies and general approaches taken by HIPAA Security Liaisons in their Security Procedures.
   b) The HIPAA Security Officer will develop and recommend to the HIPAA Security Committee any necessary Security Policy or Security Procedure changes.

3) **Periodic Evaluation by the Covered Entity HIPAA Security Committee**

   a) The HIPAA Security Committee will reconvene as needed to evaluate the technical and non-technical viability of the Covered Entity Security Policies. It is the responsibility of the Covered Entity Security Officer to reconvene the HIPAA Security Committee in accordance with this Policy.
   b) Any member of the HIPAA Security Committee, the HIPAA Security Officer, any HIPAA Security liaison or any other person may suggest changes to the Security Policies or Procedures by submitting such suggestion to the HIPAA Security Committee for consideration.
   c) The HIPAA Security Committee will review any suggested Security Policy or Security Procedure change and make a preliminary recommendation.

d) If the Security Committee preliminarily recommends a new security standard or a change in the Covered Entity's Security Policies or Procedures, such new standard or change will be communicated to the Departments by the Security Liaisons, who will elicit feedback for a specific period of time and provide such feedback to the HIPAA Security Committee.

e) The HIPAA Security Committee will consider the feedback received and make a final recommendation on the suggested change to the HIPAA Security Officer.

f) If the Covered Entity implements the change, such change will be propagated to the Departments through HIPAA Security Liaisons and the Security Officer via policy updates and reminders. Each HIPAA Security Liaison and the Security Officer will be required to update their Security Procedure in a timely manner to incorporate the change.

4) **Evaluation upon Occurrence of Certain Events**

a) In the event that one or more of the following events occur, the policy evaluation process described in Paragraph 3 will be immediately triggered:

i. Changes in the HIPAA Security Regulations or Privacy Regulations
ii. New federal, state, or local laws or regulations affecting the privacy or security of PHI
iii. Changes in technology, environmental processes or business processes that may affect HIPAA Security Policies or Security Procedures
iv. A serious security violation, breach, or other security incident occurs

b) The HIPAA Security Officer may reconvene the HIPAA Security Committee if deemed necessary based on information received from, but not limited to, the HIPAA Compliance Office, Internal Audit, a HIPAA Security Committee Member, or the HIPAA Steering Committee.

5) **Evaluation of Department Procedures by HIPAA Security Liaisons**. Each HIPAA Security Liaison and the Security Officer must periodically evaluate its HIPAA Security Procedures to ensure that such Procedures maintain their technical and non-technical viability and continue to comply with the HIPAA Security Policies.

FACILITY ACCESS CONTROL POLICY

I. POLICY

The Covered Entity shall select and implement policies and procedures to safeguard all facilities, systems, and equipment used to store EPHI against unauthorized physical access, tampering, or theft.

Maintenance should be contacted for repairs. Covered Entity shall document and manage repairs and modifications to the physical security components of the facility.

Covered Entity will verify the identity of each employee performing administrative functions on behalf of Covered Entity or other Individual prior to granting physical access to Covered Entity's information systems that contain ePHI.

II. PURPOSE

The purpose of this policy is to ensure that Covered Entity implements physical security measures that are sufficient to secure the facilities from unauthorized physical access, tampering, and theft.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(a)(2)(ii)
- 45 C.F.R. §164.310(a)(2)(iii)
- 45 C.F.R. §164.310(a)(2)(iv)
- Authorization and/or Supervision Policy
- Risk Analysis Policy
- Risk Management Policy
- Evaluation Policy

IV. PROCEDURES

A. Facility Security Plan

1) The Facility Security Plan includes the following components:

   a) Contingency Operations – procedures that allow physical facility access during emergencies to support restoration of data under a Disaster Recovery Plan.
   b) Access Control and Validation – procedures to control and validate a workforce member's access to facilities based on their role or function. This is done by Covered Entity IDs and by visual recognition of staff.
   c) Physical Access Records – procedures to log physical access to any facility containing medium and high risk EPHI-based systems. Examples of facilities requiring physical access records are computer and system rooms. This is done by sign in sheets.
   d) Maintenance Records – procedures to document and manage repairs and modifications to the physical security components of the facility including

locks, doors, and other physical access control hardware. This is done by documenting all repairs and modifications.

2) Procedures have been established and implemented to control and validate workforce member access to all facilities used to house EPHI based systems.

   a) All workforce members must wear their Covered Entity Identification Badges at all times when at work if determined appropriate by the HIPAA Security Liaison and the Security Officer.
   b) A physical access control mechanism is utilized to control physical access to all facilities containing EPHI-based systems. Code locks, badge readers, and key locks are examples of physical access control mechanisms.

3) Procedures have been established and implemented to control, validate, and document visitor access to any facility used to house EPHI based systems. This procedure applies to vendors, repair personnel, or other non-workforce members accessing such areas as server rooms etc.

   a) All visitors requiring access to facilities containing EPHI-based systems must sign in providing information regarding their identity and the purpose of their visit.
   b) All visitors must be provided a temporary identification badge or be escorted to and from their destination.

PHYSICAL SAFEGUARDS WORKSTATION USE POLICY

I. POLICY

The workstations and other computer systems that may be used to send, receive, store or access EPHI must be used in a secure and legitimate manner.

II. PURPOSE

The purpose of this policy is to establish guidelines for the permitted uses (including the proper functions to be performed and the manner in which such functions are to be performed) of workstations of employees performing administrative functions on behalf of Covered Entity and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(b)
- Workstation Security Policy

IV. PROCEDURES

1) Compliance with the Covered Entity Computer Use Policy

To ensure that workstations and other computer systems that may be used to send, receive, store or access EPHI are only used in a secure and legitimate manner, Workforce members who, and workstations and other computer systems that are used to, send, receive, store and access EPHI must comply with the Covered Entity Computer Use Employee Handout, a copy of which is attached hereto.

2) The Covered Entity Monitoring of Workstation Use

Workforce members that use the Covered Entity information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, the Covered Entity may log, review, or monitor any data (EPHI and non-EPHI) stored or transmitted on its information system assets.

3) Removal of Workforce Members Privileges

The Covered Entity may remove or deactivate any Workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

ATTACHMENT TO PHYSICAL SAFEGUARDS WORKSTATION USE POLICY

The Covered Entity Computer Use Employee Handout

Introduction

This document provides guidelines for appropriate use of computer facilities and services at the Covered Entity. It is not a comprehensive document covering all aspects of computer use. It offers principles to help guide members of the Covered Entity community, and specific policy statements that serve as reference points. It will be modified as new questions and situations arise.

While the proliferation of computers and information technologies does not alter basic codes of behavior, it does place some issues in new contexts. Using these technologies enables people to do varied things-both good and bad-more easily. They are an enormously rich resource for innovation in the furtherance of the Covered Entity's mission. But they increase the risks of actions, deliberate or not, that are harmful in various ways, including:(a) interference with the rights of others; (b) violation of the law; (c) interference with the mission of the Covered Entity; or (d) endangering the integrity of the Covered Entity's information computer network. The guidelines that follow seek to forge the link between established codes of conduct and the use of new technologies. Computer networking has greatly expanded our ability to access and exchange information, requiring more vigilant efforts and perhaps more secure safeguards to protect Individuals' rights of privacy. Property as well as privacy rights may be infringed whenever files or data belonging to others, however gained, are used without authorization; moreover, while freedom of inquiry and expression are fundamental principles of life, assaults upon the personal integrity of Individual members of the community and dissemination of offensive materials may undermine the foundations of that community. Other actions taken by Individuals may, under some circumstances, jeopardize the integrity of the computer network and the ability of others to communicate using this system. Accordingly, the guidelines that follow seek to both preserve the freedom to inquire and share information and sustain the security and integrity of Individuals within the community and the computer system itself.

While some of the guidelines therefore call for respectful and responsible use of the computer networks to protect the rights of Individuals, others warn against actions that may violate the law: users within the community must understand the perils of illegal use, exchange, or display of copyrighted, deceptive, defamatory, or obscene materials on a web page or through other electronic communication channels.

The community at large has rights and expectations that must be considered. When Individuals misrepresent either themselves or the Covered Entity, or when they act by computer in a manner unacceptable within the Covered Entity or in the larger community, the integrity and mission of the Covered Entity itself is endangered.

Finally, the guidelines seek to protect the integrity of the Covered Entity information systems themselves: the computing or networking resources need to be accessible and secure for appropriate uses consistent with the mission of the Covered Entity; the usurpation of these resources for personal gain or without authorization is unacceptable. Moreover, even the Individual right to privacy may, when personal files may need to be accessed for troubleshooting purposes, be overridden by authorized personnel to protect the integrity of the Covered Entity's computer systems.

Principles and Guidelines

A. Respect the rights and sensibilities of others

1. Electronic mail should adhere to the same standards of conduct as any other form of mail. Respect others you contact electronically by avoiding distasteful, inflammatory, harassing or otherwise unacceptable comments.
2. Others have a right to know who is contacting them.
3. Respect the privacy of others and their accounts. Do not access or intercept files or data of others without permission. Do not use the password of others or access files under false identity.
4. Distribution of excessive amounts of unsolicited mail is not allowed.
5. While the Covered Entity encourages respect for the rights and sensibilities of others, it cannot protect Individuals against the existence or receipt of materials that may be offensive to them. Those who make use of electronic communications may come across or be recipients of material they find offensive or simply annoying.

B. Be aware of the legal implications of your computer use.

1. The Internet enables users to disseminate material worldwide. Thus, the impact of dissemination on the internet is often far broader than that of a statement made on paper or in routine conversation. Keep in mind that a larger audience means a greater likelihood that someone may object with or without legal basis.
2. Much of what appears on the internet is protected by copyright law regardless of whether the copyright is expressly noted. Users should generally assume that material is copyrighted unless they know otherwise and not copy or disseminate copyrighted material without permission. Copyright protection also applies to much software, which is often licensed to the Covered Entity with specific limitations on its use. Both Individual users and the Covered Entity may, in some circumstances, be held legally responsible for violations of copyright.
3. Many other state and federal laws, including those prohibiting deceptive advertising, use of others' trademarks, defamation, violations of privacy, and obscenity apply to network-based communications.

C. Respect the mission of the Covered Entity in the larger community

1. The Covered Entity makes internet resources available to staff to further the Covered Entity's service and related missions. While incidental personal use is permissible in most settings, these resources are generally available only for Covered Entity-related activities.
2. The Covered Entity may monitor the content of web pages, electronic mail or other on-line communications. Under certain circumstances, the Covered Entity may be held liable if it fails to take reasonable remedial steps after it learns of illegal uses of its computer facilities. Use computer resources lawfully.
3. Remember that you are responsible for all activity involving your account. Keep your account secure and private. Your password should be difficult to crack or otherwise guess either by Individuals or by sophisticated computer programs.
4. The Covered Entity is the custodian of a wide array of personal and financial data concerning its staff and clients, as well as the Covered Entity itself. Respect the Covered Entity obligations of confidentiality as well as your own. Only those with authorization may access, communicate or use confidential information.

5. Material posted on WEB pages is generally accessible and thus deserves even greater thought and care than your private electronic mail. Remember that, absent restrictions, your web page is available to anyone, anywhere, and act accordingly.
6. The Covered Entity has a right to expect that computer users will properly identify themselves. Computer accounts are assigned and identified to Individuals. Don't misrepresent yourself.

D. Do not harm the integrity of the Covered Entity's computer systems and networks.

1. Today's information technology is a shared resource. Respect the needs of others when using computer and network resources. Do not tamper with facilities and avoid any actions that interfere with the normal operations of computers, networks, and facilities.
2. Avoid excessive use of computer resources. They are finite and others deserve their share. Chain mail, junk mail, and similar inappropriate uses of Covered Entity resources are not acceptable. Web pages that are accessed to an excessive degree can be a drain on computer resources and, except where significant to the Covered Entity's mission, may require the Covered Entity to ask that they be moved to a private Internet provider.
3. Although a respect for privacy is fundamental to the Covered Entity's policies, understand that almost any information can in principle be read or copied; that some user information is maintained in system logs as a part of responsible computer system maintenance; that the Covered Entity must reserve the right to examine computer files, and that, in rare circumstances, the Covered Entity may be compelled by law or policy to examine even personal and confidential information maintained on Covered Entity computing facilities.
4. You are granted privileges and responsibilities with your account. While these vary between groups, the use of Covered Entity resources for personal commercial gain or for partisan political purposes is inappropriate and possibly illegal.
5. Individual Covered Entity computer systems have varying resources and demands. Some have additional and sometimes more restrictive guidelines applicable to their own user.

Implementation

1. All Covered Entity codes of conduct apply to information technology as well as to other forms of communication and activity.
2. Systems managers or other Individuals within a department may be empowered to suspend some or all privileges associated with computer use in cases of misuse or threat to the integrity of all or part of the Covered Entity's information management resources.
3. Before any permanent action is taken against a user, the user will be advised of the basis for the proposed action and given an opportunity to respond. Concerns about such actions may be raised through the usual administrative channels associated with the department or resource in question.
4. Where a violation of Covered Entity policies or applicable law appears to warrant action beyond a suspension or elimination of computer privileges, the matter may be referred to a supervisor, administrator or Covered Entity disciplinary body with appropriate authority or to law enforcement authorities.
5. Complaints or concerns about another's use of Covered Entity computer resources should be directed to the administrator responsible for the resource in question.

SERVER, WORKSTATION, AND MOBILE SYSTEMS SECURITY POLICY

I. POLICY

Covered Entity will implement physical safeguards to protect workstations that contain EPHI from unauthorized access.

II. PURPOSE

The purpose of this policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store EPHI to ensure that appropriate security is maintained, and that access is restricted to authorized users.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(c)
- Workstation Use Policy

IV. PROCEDURES

1) **General Security Requirements**. The Security Officer will ensure each server, desktop computer system and wireless computer system used to access, transmit, receive and store EPHI to ensure that appropriate security is maintained, and that access is restricted to authorized users. Each workstation that is used to access, transmit, receive or store EPHI must comply with each of the aforementioned measures. If any of the aforementioned measures are not supported by the workstation operating system or system architecture, one of the following steps must be taken:

   a) The server, desktop computer system, or wireless computer system must be upgraded to support all of the following security measures,
   b) An alternative security measure must be implemented and documented, or
   c) The workstation must not be used to send, receive or store EPHI.

2) **Server Security Requirements**

   a) Each HIPAA Security Liaison and the Security Officer must ensure that all servers used to access, transmit, receive or store EPHI are appropriately secured in accordance with this Policy.
   b) Servers must be located in a physically secure environment.
   c) The system administrator or root account must be password protected.
   d) A user identification and password authentication mechanism must be implemented to control user access to the system.
   e) A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected
   f) Servers must be located on a secure network with firewall protection. If for any reason the server must be maintained on a network that is not

secure, an intrusion detection system must be implemented on the server to detect changes in operating and file system integrity.

g) All unused or unnecessary services shall be disabled.

3) **Desktop System Security Requirements**

a) Each HIPAA Security Liaison and the Security Officer must ensure that each desktop system used to access, transmit, receive or store EPHI is appropriately secured in accordance with this Policy.

b) The system administrator or root account must be password protected.

c) A user identification and password authentication mechanism must be implemented to control user access to the system.

d) A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

e) A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.

f) All unused or unnecessary services must be disabled.

g) Desktop systems that are located in open, common, or otherwise insecure areas must also implement the following measures:

i. An inactivity timer or automatic logoff mechanism must be implemented.

ii. The workstation screen or display must be situated in a manner that prohibits unauthorized viewing.

4) **Mobile Systems Security Policy**

a) Each HIPAA Security Liaison and the Security Officer must ensure that all mobile systems used by Workforce Members to access, transmit, receive or store EPHI are appropriately secured in accordance with this Policy.

b) The system administrator or root account must be password protected.

c) A user identification and password authentication mechanism must be implemented to control user access to the system. All mobile devices and laptops must use a boot password to ensure that the system is only accessible to authorized users.

d) A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

e) A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up-to-date.

f) All unused or unnecessary services must be disabled.

g) Mobile stations that are located or used in open, common, or otherwise insecure areas must also implement the following measures:

i. A theft deterrent device such as a laptop locking cable must be utilized when the device is unattended.

ii. An inactivity timer or automatic logoff mechanism must be implemented.

iii. Reasonable safeguards must be in place to prohibit unauthorized entities from viewing confidential information.

h) Each mobile system that is used to access, transmit, receive, or store EPHI must comply with as many of the aforementioned measures as is allowed by the system and operating system architecture.

PHYSICAL SAFEGUARDS DEVICE AND MEDIA CONTROLS POLICY

I. POLICY

The purpose of this policy is to establish guidelines for the secure disposal of electronic media containing ePHI

II. PURPOSE

The purpose of this policy is to establish guidelines for the secure disposal of electronic media containing EPHI.

This policy outlines the policy and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility and the movement of such items within the facility.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.310(d)(2)(i)
- 45 C.F.R. §164.310(d)(2)(ii)
- 45 C.F.R. §164.310(d)(2)(iii)

IV. PROCEDURES

1) **General Application of Policy**

a) These policies and procedures pertain to the use of hard drives, storage systems, removable disks, floppy drives, CD ROMs, PCMCIA cards, memory sticks, and all other forms of removable media and storage devices.

b) The procedures developed pursuant to this Policy must be documented and submitted to the HIPAA Security Officer for approval.

2) **Destruction of Storage Devices or Removable Media**

a) Prior to destroying or disposing of any storage device or removable media, care must be taken to ensure that the device or media does not contain EPHI.

b) If the device or media contains the only copy of EPHI that is required or needed, a retrievable copy of the EPHI must be made prior to disposal.

c) If the device or media contains EPHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal.

d) In the event EPHI is disposed of, it shall be disposed destroyed in a manner approved of by the Secretary.

3) **Reuse of Storage Devices or Removable Media**

a) Prior to making storage devices and removable media available for reuse, care must be taken to ensure that the device or media does not contain EPHI.

b) If the device or media contains the only copy of EPHI that is required or needed, a retrievable copy of the EPHI must be made prior to reuse.

c) If the device or media contains EPHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse.

d) If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, the use of a data destruction tool between uses is not necessary.

4) **Movement of Equipment Housing EPHI**

a) Each Department shall develop a procedure to determine when an exact retrievable copy of EPHI is required prior to the movement of equipment storing such EPHI.

b) When using storage devices and removable media to transport EPHI each Department must develop a procedure to track and maintain records of the movement of such devices and the media and the parties responsible for the device and media during its movement.

ACCESS CONTROL POLICY

I. POLICY

Covered Entity will assign a unique name and/or number to each employee performing administrative functions on behalf of Covered Entity that is authorized to access ePHI and will maintain a user authentication procedure.

Covered Entity will safeguard ePHI through the use of automatic log off technology that terminates or suspends an electronic session after a predetermined time (15 minutes) of inactivity.

II. PURPOSE

The purpose of this policy is to ensure that authorized users are granted the level of access to information and data appropriate to their job assignments or functions and that unauthorized users are prevented from accessing any data. Assigning a unique name and/or number allows the system administrator to be able to identify and track users on the system. The purpose of this policy is also to mitigate the risk that an unauthorized user may use an authorized user's account after the authorized user has logged in.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(a)(2)(i)
- 45 C.F.R. §164.312(a)(2)(iii)
- 45 C.F.R. §164.312(e)
- Password Management Policy
- Workstation Use Policy
- Server, Desktop, and Wireless Computer System Security Policy

IV. PROCEDURES

1) **Unique User Identification**. To uniquely identify and track one user or workforce member from all others, for the purpose of access control to all networks, systems, and applications that contain EPHI, and the monitoring of access to the aforementioned networks, systems, and applications, the following procedures must be implemented:

   a) Any user or workforce member that requires access to any network, system, or application that accesses, transmits, receives, or stores EPHI, must be provided with a unique User Identification string.
   b) When requesting access to any network, system, or application that accesses, transmits, receives, or stores EPHI, a user or workforce member must supply their previously assigned unique User Identification in conjunction with a secure password to gain access to the aforementioned networks, systems, or applications.
   c) Users or workforce members must not allow another user or workforce member to use their unique User Identification or Password.

d) Users or workforce members must ensure that their Password is not documented, written, or otherwise exposed in an insecure manner unless it is to be hard coded into the system in which case it will be shared with the appropriate IT personnel.

2) **Firewall Use**. All networks housing EPHI repositories must be appropriately secured. To ensure that all networks that contain EPHI based systems and applications are appropriately secured, the following policies and procedures are followed:

a) Networks containing EPHI-based systems and applications must implement perimeter security and access control with a firewall.

b) Firewalls must be configured to support the following minimum requirements:

i. Limit network access to only authorized workforce members and entities.
ii. Limit network access to only legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
iii. Console and other management ports must be appropriately secured or disabled.
iv. Implement mechanism to log failed access attempts.
v. Must be located in a physically secure environment.

c) The configuration of firewalls used to protect networks containing EPHI-based systems and applications must be documented internally by the Security Officer [and each HIPAA Security Liaison]. This documentation should include a configuration plan that outlines and explains the firewall rules.

d) The configuration of firewalls used to protect networks containing EPHI-based systems and applications must be submitted to and approved by the HIPAA Security Officer.

3) **Wireless Access**. To ensure that all networks that contain EPHI based systems and applications are appropriately secured, the following wireless access policies and procedures must be followed:

a) Wireless access to networks containing EPHI-based systems and applications is permitted so long as the following security measures have been implemented:

i. Encryption must be enabled.
ii. MAC-based or User ID/Password authentication must be enabled.
iii. All console and other management interfaces have been appropriately secured or disabled.

b) Unmanaged, ad-hoc, or rogue wireless access points are not permitted on any secure network containing EPHI-based systems and applications.

c) All wireless LANs do not utilize standard 2.4 GHz, 5.0 GHz or microwave radio frequencies. Wireless LANs and devices may utilize infrared frequencies and may not support the typical wireless LAN encryption and security mechanisms. For instance, the use of infrared ports on PDAs, laptops, and printers to transmit EPHI may not allow encryption of that data stream. This is a low risk concern because this implementation of infrared is very short distance and low power.

4) **Remote Access**. To ensure that all networks that contain EPHI based systems and applications are appropriately secured, the following remote access policies and procedures must be followed:

a) Dialup connections directly into secure networks are considered to be secure connections and do not require a VPN connection.

b) Authentication and encryption mechanisms are required for all remote access sessions to networks containing EPHI via an Internet service provider or dialup connection. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, etc.

c) The following security measures must be implemented for any remote access connection into a secure network containing EPHI:

i. Mechanisms to bypass authorized remote access mechanisms are strictly prohibited.

ii. Remote access systems must employ a mechanism to "clear out" cache and other session information upon termination of session

iii. Remote access workstations must employ a virus detection and protection mechanism

iv. Users of remote workstations must comply with the HIPAA Security Workstation Use Policy

d) VPN split-tunneling is not permitted for connections originating from outside the Covered Entity network or from an insecure network within the Covered Entity domain.

e) The HIPAA Security Liaison of any workforce member requesting remote access to a secure network containing EPHI-based systems and applications must ensure that the remote workstation device being used by said workforce member meets the security measures detailed in the HIPAA Security Server, Desktop, and Wireless Computer System Security Policy. The owner of the secure network must ensure that the previous requirement has been satisfied before access is granted.

f) The Security Officer and each HIPAA Security Liaison must establish a formal, documented procedure to ensure that remote workstations and mobile devices used by their workforce members to remotely access secure networks containing EPHI-based systems and applications continue to meet the security measures detailed in the Server, Desktop, and Wireless Computer System Security Policy.

5) **Automatic Logoff**. To ensure that access to all servers and workstations that access, transmit, receive, or store EPHI is appropriately controlled, the following procedures must be followed:

a) Servers, workstations, or other computer systems containing EPHI repositories must employ inactivity timers or automatic logoff mechanisms. The aforementioned systems must terminate a user session after a maximum of, but not limited to, 15 minutes of inactivity.

b) Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit, receive, or store EPHI must employ inactivity timers or automatic logoff mechanisms. (I.E. Password protected screen saver that blacks out screen activity.) The aforementioned systems must terminate a user session after a maximum of, but not limited to, 15 minutes of inactivity.

c) Applications and databases using EPHI, such as Electronic Medical Records (EMR), must employ inactivity timers or automatic session logoff mechanisms. The aforementioned application sessions must automatically terminate after a maximum of, but not limited to, 15 minutes of inactivity.

d) Servers, workstations, or other computer systems that access, transmit, receive, or store EPHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.

e) If a system requires the use of an inactivity timer or automatic logoff mechanism as detailed in the aforementioned procedures, but does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:

i. The system must be upgraded or moved to support the minimum HIPAA Security Automatic Logoff procedures.
ii. The system must be moved into a secure environment.
iii. All EPHI must be removed and relocated to a system that supports the minimum HIPAA Security Automatic Logoff procedures.

f) When leaving a server, workstation, or other computer system unattended, workforce members must lock or activate the systems Automatic Logoff Mechanism or logout of all applications and database systems containing EPHI.

6) **Encryption**. The implementation of the aforementioned policies will ensure that access to EPHI and its associated applications, systems, and networks are appropriately secured and controlled. Encryption of EPHI as an access control mechanism is not required unless the custodian of said EPHI deems the data to be highly critical or sensitive. Encryption of EPHI is required in some instances as a transmission control and integrity mechanism.

TECHNICAL SAFEGUARDS AUDIT CONTROLS POLICY

I. POLICY

With the exception of emails, Covered Entity will employ audit controls and audit trail capabilities to record and examine activity in the system.

II. PURPOSES

The purpose of this policy is to ensure that hardware, software, and/or procedural mechanisms will be implemented by the Covered Entity Departments, and to record and examine activity in information systems that contain or use EPHI.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(b)
- General Information System Activity Review Policy

IV. PROCEDURES

1) **Audit Control Mechanisms**

a) Each HIPAA Security Liaison and the Security Officer with systems containing medium and high risk EPHI must utilize a mechanism to log and store system activity.
b) Each system's audit log must include, but is not limited to, User ID, Login Date/Time, and Activity Time. Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.
c) System audit logs must be reviewed on a regular basis.
d) Implementation of an audit control mechanism for systems containing low risk EPHI is not required.

2) **Audit Control and Review Plan**

a) An Audit Control and Review Plan must be developed by each HIPAA Security Liaison and the Security Officer. If the Department's EPHI inventory changes, its Audit Control and Review Plan must be reevaluated and resubmitted to the HIPAA Security Officer. The plan must include:

i. Systems and applications to be logged
ii. Information to be logged for each system
iii. Log-in reports for each system
iv. Procedures to review all audit logs and activity reports

These procedures are covered in the Risk Analysis, Emergency Mode Operations, and Data Disaster Recovery Plan for each covered department, which is attached.

INTEGRITY AND AUTHENTICATION POLICY

I. POLICY

Covered Entity will review whether EPHI maintained on Covered Entity's systems has been altered or destroyed in an unauthorized manner. Covered Entity will educate those with access to EPHI not to alter or destroy EPHI in an unauthorized manner.

II. PURPOSES

The purpose of this policy is to ensure that EPHI maintained on Covered Entity's systems has not been altered or destroyed in an unauthorized manner.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(c)(2)
- Data Back Up Plan Policy
- HIPAA Security Transmission Policy

IV. PROCEDURES

1) The following mechanisms will ensure the Covered Entity

   a) A mechanism to corroborate that EPHI is not altered or destroyed in an unauthorized manner.
   b) A mechanism for all systems containing EPHI to ensure that EPHI has not been altered or destroyed by a virus or other malicious code.
   c) Error-correcting memory and storage mechanism to authenticate data storage and retrieval

2) EPHI is backed up in accordance with the Data Back Up Plan Policy.

3) Covered Entity will train employees not to alter or destroy EPHI in an unauthorized manner.

4) In monitoring use of EPHI, Covered Entity will review and respond to any indication of alteration.

5) For high risk EPHI, a DES (Digital Encryption Standard) encryption mechanism or data checksum can be used to ensure the integrity of data at rest. The use of data authentication mechanisms other than virus detection is not required for low risk EPHI.

These procedures are covered in the Risk Analysis, Emergency Mode Operations, and Data Disaster Recovery Plan for each covered department, which is attached.

PERSON OR ENTITY AUTHENTICATION POLICY

I. POLICY

Covered Entity will authenticate all persons seeking access to its EPHI and will restrict internal and external access to EPHI to authorized entities.

II. PURPOSE

The purpose of this policy is to verify the identity of the persons and entities seeking access to EPHI. This Policy covers the procedures to be implemented by the Covered Entity's Security Officer and the HIPAA Security Liaison to verify that a person or entity seeking access to EPHI is the person or entity claimed.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(d)
- Unique User Identification Policy
- Password Management Policy

IV. PROCEDURES

1) Covered Entity will review EPHI access on a monthly basis.

2) The persons and entities authorized to access EPHI are listed in the Access Control List, all as set out in the Unique User Identification Policy.

3) Workforce members seeking access to any network, system, or application that contains EPHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity, all in accordance with the applicable policies adopted by Covered Entity.

4) Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.

5) Workforce members are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.

6) A reasonable effort must be made to verify the identity of the receiving person or entity prior to transmitting EPHI.

7) System and Security administrators will configure the system to ensure that:

   a) Passwords include security control features to prevent hacking, such as randomization, required password structure (upper and lower case; numbers and letters), non-commonality with personal information, etc.

b) Users change their passwords in accordance with the Password Management Policy.

c) A user ID locks after failed log-in attempts in accordance with the Unique User Identification Policy.

d) The Access Control List is subject to access protection or one-way encryption.

TECHNICAL SAFEGUARDS TRANSMISSION SECURITY POLICY

I. POLICY

Covered Entity will safeguard EPHI that is transmitted electronically against loss, alteration, duplication, substitution, or destruction.

II. PURPOSE

This Policy covers the technical security measures that the Security Officer and each HIPAA Security Liaison will implement to guard against unauthorized access to or modification of EPHI that is being transmitted over an electronic communications network or via any form of removable media.

III. REFERENCES/CROSS REFERENCES

- 45 C.F.R. §164.312(a)(2)(iv)
- 45 C.F.R. §164.312(e)

IV. PROCEDURES

1) **EPHI Transmissions to Non-the Covered Entity Entities**

   a) To appropriately guard against unauthorized access to or modification of EPHI that is being transmitted from the Covered Entity domains to a network outside of such networks, the procedures outlined in this Paragraph must be implemented.

   b) All transmissions of EPHI from the Covered Entity domains to a network outside of the aforementioned networks must utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing said EPHI must be encrypted before transmission or must be password protected.

   c) Prior to transmitting EPHI from the Covered Entity domains to a network outside of the aforementioned networks the receiving person or entity must be authenticated.

   d) All transmissions of EPHI from the Covered Entity domains to a network outside of the aforementioned networks should include only the minimum amount of PHI.

   e) For transmission of EPHI from the Covered Entity domains to a network outside of the aforementioned networks utilizing an email or messaging system, see Paragraph 4 below.

2) **EPHI Transmission between the Covered Entity Entities**

   a) When transmitting EPHI over an electronic network between the Covered Entity entities, the EPHI must be password protected or encrypted before transmission as described below.

   b) All transmissions of EPHI from the Covered Entity domain must utilize an encryption mechanism or be password protected.

c) All transmissions from the Covered Entity that do not contain EPHI require no additional security mechanisms.

3) **EPHI Transmissions Using Electronic Removable Media**

a) When transmitting EPHI via removable media, including but not limited to, floppy disks, CD ROM, memory cards, magnetic tape and removable hard drives, the sending party must:

i. Use an encryption mechanism or password to protect against unauthorized access or modification
ii. Authenticate the person or entity requesting said EPHI in accordance with the Person or Entity Authentication Policy.
iii. Send the minimum amount of said EPHI required by the receiving person or entity.

b) If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, no additional security mechanisms are required.

4) **EPHI Transmissions Using Email or Messaging Systems**

a) The transmission of EPHI from the Covered Entity to a client via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

i. The client has been made fully aware of the risks associated with transmitting EPHI via email or messaging systems.
ii. The client has formally in writing or through email authorized the Covered Entity to utilize an email or messaging system to transmit EPHI to them.
iii. The client's identity has been authenticated.
iv. The email or message contains no excessive history or attachments.

b) The transmission of EPHI from the Covered Entity to an outside entity via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

i. The receiving entity has been authenticated.
ii. The receiving entity is aware of the transmission and is ready to receive it.
iii. The sender and receiver are able to implement a compatible encryption mechanism or password.
iv. All attachments containing EPHI are encrypted or password protected.

c) The transmission of EPHI within the Covered Entity via an email or messaging system is permitted without additional security measures or safeguards so long as only a minimal amount of EPHI is being transmitted and the EPHI is not high risk, sensitive or critical. EPHI that is high risk, sensitive or critical should not be sent through clear text email; such EPHI should be sent via encrypted attachment or other secure measure as described in paragraph 4(b) above. If an email or message includes an attachment that contains EPHI, the attachment must be encrypted or password protected before transmission.

d) Email accounts that are used to send or receive EPHI must not be forwarded to non-the Covered Entity accounts.

5) **EPHI Transmissions Using Email or Messaging Systems**

a) The transmission of EPHI over a wireless network within the Covered Entity domains is permitted if the following conditions are met:

i. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.

ii. The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network.

b) If transmitting EPHI over a wireless network that is not utilizing an authentication and encryption mechanism, the EPHI must be encrypted before transmission.

c) The authentication and encryption security mechanisms implemented on wireless networks within the Covered Entity domains are only effective within those networks. When transmitting outside of those wireless networks, additional and appropriate security measures must be implemented in accordance with this Policy.

6) **Additional Requirements**

a) When transmitting EPHI electronically, regardless of the transmission system being used, Workforce members must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the EPHI requested.

b) If the EPHI being transmitted is not to be used for treatment, payment or health care operations, only the minimum required amount of PHI should be transmitted.

APPENDIX A
GLOSSARY

Act means the Social Security Act.

ANSI stands for the American National Standards Institute.

Business associate: means any entity or person who, on behalf of Covered Entity (but other than in the capacity of a member of the Covered Entity's workforce), creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, Individual safety activities, billing, benefit management, practice management, and repricing, or Uses PHI to provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Covered Entity. It includes a health information organization, e-prescribing gateway or other entity or person who provides data transmission services with respect to PHI and that requires access on a routine basis to such PHI. It does not, however, include an officer, director, or employee of Covered Entity. It includes a person that offers a personal health record on behalf of the Covered Entity. It includes a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity would find it impossible to comply with both the State and federal requirements; or
(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody include juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered entity means:

(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to PHI created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such PHI by the business associate with the PHI received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

De-identification of PHI. A covered entity may determine that health information is not Individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not Individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an Individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2) (i) The following identifiers of the Individual or of relatives, employers, or household members of the Individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, Covered Entity, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an Individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an Individual who is a subject of the information.

Designated record set refers to (1) the medical records and billing records about Individuals maintained by or for Covered Entity, or (2) any item, group, or collection of information that includes PHI and is used in whole or in part by or for Covered Entity to make decisions about Individuals.

Direct treatment relationship means a treatment relationship between an Individual and a health care provider that is not an indirect treatment relationship.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury.

The EIN is the taxpayer identifying number of an Individual or other entity (whether or not an employer) assigned under one or the following:

(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.
(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.

Employer is defined as it is in 26 U.S.C. 3401(d).

Group health plan (also see definition of health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
(2) Is administered by an entity other than the employer that established and maintains the plan.

HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an Individual.

Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an Individual or that affects the structure or function of the body; and
(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with paragraph (c)(3)(iii) of this section.

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and Individuals with information about treatment alternatives; and related functions that do not include treatment;
(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;
(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
(6) Business management and general administrative activities of the entity, including, but not limited to:
(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer.
(iii) Resolution of internal grievances;
(iv) the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan in this section) means a federally

qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health plan means an Individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) Health plan includes the following, singly or in combination:
(i) A group health plan, as defined in this section.
(ii) A health insurance issuer, as defined in this section.
(iii) An HMO, as defined in this section.
(iv) Part A or Part B of the Medicare program under title XVIII of the Act.
(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g) (1) of the Act, 42 U.S.C. 1395ss (g) (1)).
(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
(viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
(ix) The health care program for active military personnel under title 10 of the United States Code.
(x) The veterans' health care program under 38 U.S.C. chapter 17.
(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).
(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.
(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
(xv) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
(xvi) A high-risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible Individuals.
(xvii) Any other Individual or group plan, or combination of Individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) Health plan excludes:
(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg- 91(c)(1); and
(ii) A government-funded program (other than one listed in paragraph (1) (i)-(xvi) of this definition):
(A) Whose principal purpose is other than providing, or paying the cost of, health care; or
(B) Whose principal activity is:
(1) The direct provision of health care to persons; or
(2) The making of grants to fund the direct provision of health care to persons.

Hybrid entity means a single legal entity:
(1) That is a covered entity;
(2) Whose business activities include both covered and non-covered functions; and
(3) That designates health care components in accordance with paragraph (c) (3) (iii) of this section.

Implementation specification means specific requirements or instructions for implementing a standard.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an Individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and
(i) That identifies the Individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

Indirect treatment relationship means a relationship between an Individual and a health care provider in which:

(1) the health care provider delivers health care to the Individual based on the orders of another health care provider; and
(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the Individual.

Individual means the person who is the subject of PHI.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or
(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited data set: A limited data set is PHI that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual:

(i) Names;
(ii) Postal address information, other than town or city, State, and zip code;
(iii) Telephone numbers;
(iv) Fax numbers;
(v) Electronic mail addresses;
(vi) Social security numbers;
(vii) Medical record numbers;
(viii) Health plan beneficiary numbers;
(ix) Account numbers;
(x) Certificate/license numbers;
(xi) Vehicle identifiers and serial numbers, including license plate numbers;
(xii) Device identifiers and serial numbers;
(xiii) Web Universal Resource Locators (URLs);
(xiv) Internet Protocol (IP) address numbers;
(xv) Biometric identifiers, including finger and voice prints; and
(xvi) Full face photographic images and any comparable images.

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the Individual, only if any payment received in exchange for making the communication is reasonably related to the cost of making the communication.
(ii) For the following purposes, except where [INSERT NAME] receives payment in exchange for making the communication:
(A) For treatment of an Individual, including case management or care coordination for the Individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the Individual;
(B) To describe a health-related product or service (or payment for such product or service) that is provided by [INSERT NAME]; or
(C) For case management or care coordination, contacting of Individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

Modify or modification refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:
(i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or
(ii) To the Individual who is the subject of the Individually identifiable health information.
(2) With respect to the rights of an Individual, who is the subject of the Individually identifiable health information, regarding access to or amendment of Individually identifiable health information, permits greater rights of access or amendment, as applicable.
(3) With respect to information to be provided to an Individual who is the subject of the Individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.
(4) With respect to the form, substance, or the need for express legal permission from an Individual, who is the subject of the Individually identifiable health information, for use or disclosure of Individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.
(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.
(6) With respect to any other matter, provides greater privacy protection for the Individual who is the subject of the Individually identifiable health information.

Organized health care arrangement means:

(1) A clinically integrated care setting in which Individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
(i) Hold themselves out to the public as participating in a joint arrangement; and
(ii) Participate in joint activities that include at least one of the following:
(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a covered

entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to PHI created or received by such health insurance issuer or HMO that relates to Individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) the group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers or HMOs that relates to Individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment means:

(1) The activities undertaken by:

(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the Individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:

(A) Name and address;
(B) Date of birth;
(C) Social security number;
(D) Payment history;
(E) Account number; and
(F) Name and address of the health care provider and/or health plan.

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Plan sponsor is defined as defined at section 3(16) (B) of ERISA, 29 U.S.C. 1002(16) (B).

PHI refers to any information, whether transmitted or maintained in electronic, written, oral, or any other form or medium, that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual; and (i) identifies the Individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual..

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the

rest of the Individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Qualified protective order means, with respect to PHI requested under paragraph (e) (1) (ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(1) Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
(2) Requires the return to the covered entity or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

Relates to the privacy of Individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

Required by law refers to a mandate contained in law, and enforceable by a court, that compels Covered Entity to use or disclose PHI. This includes, but is not limited to, court orders, subpoenas issues by a court, grand jury, or administrative body authorized to require the production of information, and civil or investigative demands.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services or practices:
(i) Classification of components.
(ii) Specification of materials, performance, or operations; or
(iii) Delineation of procedures; or
(2) With respect to the privacy of Individually identifiable health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.
(2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

Summary health information means information, that may be Individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by Individuals for whom a plan sponsor has provided health benefits under a group health plan; and
(2) From which the information described at § 164.514(b) (2) (i) has been deleted, except that the geographic information described in § 164.514(b) (2) (i) (B) need only be aggregated to the level of a five-digit zip code.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.
(2) Health care payment and remittance advice.
(3) Coordination of benefits.
(4) Health care claim status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.
(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Other transactions that the Secretary may prescribe by regulation.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to an Individual; or the referral of an Individual for health care from one health care provider to another.

Use means, with respect to Individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

CICS

Risk Analysis, Data Disaster Recovery and Emergency Mode Operations

DATA SERVICES: *Community Services* **LOCATION:** *Community Resource Center*

I. LIST OF ALL ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)

All staff have access to the Community Services Network (CSN) which is a web-based consumer data system and Office 365. A copy of the emergency data recovery plan for CSN is kept on sight in the Community services office.
Equipment Insured by: Knapp Tedesco 627 Main Street, Ames, IA 515-232-7060
Insurance documents are stored: CICS Story County Office.

II. RISK ANALYSIS See above

III. BUSINESS IMPACT ANALYSIS

A. Costs of Loss of EPHI: The cost of recreating the EPHI is minimized by the availability of CSN and Office 365. If EPHI is lost, the exposure would be in terms of damage to the reputation of the Region and possible failure to provide services. In addition, there is the possibility of costs associated with legal actions.

B. Risks: The risk of physical loss of information, both critical and sensitive, is associated with the reliability of the equipment, the power protection afforded the equipment, the security of the premises, and the age of the equipment. We have tried to minimize these risks by the following:
1. Real time connection with CSN and Office 365. As of August 2021, all counties in CICS are using OneDrive or SharePoint to store information;
2. The quality of the equipment is reasonable, within budget constraints;
3. The premises are protected with high-quality locks, fire protection, and fire detection systems.

IV. SECURITY SAFEGUARDS

All personnel are made familiar with the requirements for security and confidentiality through training.

A. Backups: Office 365 files and CSN files are kept in the cloud.

B. Paper forms used for data input, and reports associated with confidential information are kept in files which are locked when we are away from our offices. All buildings are kept locked after normal work hours, on weekends and holidays, and during periods when staff are absent from the office area. All computers in the office are password-protected and have inactive-lock time-out software installed.

C. Access to EPHI is limited to the appropriate personnel. A list of data access privileges for each job description is as follows:
CEO and Officers: Access to all files.
Program Manager and Office Managers: Access to all files.
Service Coordinators: Access to assigned client information.
Master passwords and all other passwords are changed on a 90-day cycle or more frequently if a breach of security is suspected, or the employee leaves employment.

D. The disaster recovery plan, security safeguards, access rights, and staff responsibilities are covered in our HIPAA Compliance Plan. This Plan is reviewed yearly and updated as required. All persons will be required to use a Unique ID and password meeting the minimum standards in order to access systems containing EPHI. Equipment is configured to force the expiration and changing of all passwords at least every ninety (90) days.

E. Employee security:

- No employee is to bring to work any unauthorized data storage device such as USB memory keys, external plug-in storage media such as hard disk drives, 'Zip' drives, or CD burners. Breaches of this rule will result in sanctions outlined in the HIPAA Compliance Plan up to and possibly including immediate dismissal.
- All electronic communications that contain sensitive data are password protected or encrypted.
- As soon as an employee resigns or is dismissed, the employee's access to data is terminated.
- No employee may give their passwords to any other employee or use any other employee's passwords to gain access to data.

F. Equipment Auditing:

An assigned office manager will maintain and manage an active inventory of all equipment and software. Copies are located on Office 365. All incoming equipment and software will be labeled and tracked for identification purposes.

G. Data Auditing:

Internal audit procedures have been implemented to regularly review records of information system activity, including audit logs, access reports, and security incident tracking reports.

1) An internal audit procedure has been established and implemented by the Region to regularly review records of system activity. The internal audit procedure utilizes audit logs, activity reports, and other mechanisms to document and manage system activity.

2) Audit logs, activity reports, and other mechanisms to document and manage system activity are reviewed quarterly.

3) The Audit Control and Review Plan includes the following procedures:

a) Systems and Applications to be logged: CSN and Office 365. (Note that CSN usage is also audited by ISAC.)

b) Information to be logged for each system: Each system's audit log includes; User ID, Login Date/Time, and Activity Time. Audit logs will include quarterly review of employee's current data access for up to four hours, i.e. employees will be contacted to log access and modifications to any EPHI Files.

c) The following procedures to review all audit logs and activity reports will be followed: Audit reports will be reviewed and stored for six years.

4) Security incidents such as activity exceptions and unauthorized access attempts if they occur are detected, logged and reported immediately to the assigned Assistant HIPAA Security Officer.

V. PLAN ACCURACY

This plan is tested, reviewed, and updated as required.

VI. Contact Data of Key Personnel

Name: Russell Wood CEO
Cell Phone: 641-494-9796
E-mail: Russell.wood@cicsmhds.org

Name: Christy Christenson SERVICE COORDINATOR and Assistant HIPAA Officer, Winterset
(Covers: Jasper, Madison, Marshall, Poweshiek, Story, and Warren)
Phone: 515-493-1453
E-mail: Christy.christenson@cicsmhds.org

Name: Lisa Leanhart OFFICE MANAGER and Assistant HIPAA Officer, Clarion
(Covers: Boone, Cerro Gordo, Franklin, Greene, Hamilton, Hancock, Hardin, Webster, and Wright)
Phone: 515-532-3309
E-mail: Lisa.Leanhart@cicsmhds.org

Name: Lisa Hill OFFICE MANAGER, CSN Expert User, and IT Coordinator, Hampton
Phone: 641-456-2128
E-mail: lisa.hill@cicsmhds.org

Name: Betsy Stursma, FINANCE OFFICER and CSN Expert User, Indianola
Phone: 515-961-1059
E-mail: betsy.stursma@cicsmhds.org

Name: Tanya Martinson OFFICE MANAGER and CSN Expert User, Fort Dodge
Phone: 515-573-1485
E-mail: tanya.martinson@cicsmhds.org

Name: Gabe Johanns IT DIRECTOR
Cell Phone: 641-210-5834
E-mail: gjohanns@co.franklin.ia.us
Other contact: Courthouse: 641-456-6044

Last updated on: 5/20/2022 Next update due: 6/30/2023

In the event of change to key personnel (death, disappearance, dismissal, serious injury):

Department Head: The Finance Officer is to immediately assume the temporary role of CEO until a new CEO is appointed by the Board. System passwords may be changed by the appropriate IT personnel.

HIPAA Officers will back each other up.

VII. ESSENTIAL SYSTEM INFORMATION

Backup drive type: MS Office 365

Backup software needed for data recovery: Office 365

Workstation software: Basic configuration: At least Windows 10 Professional, MS Office 365.

VIII. EMERGENCY PROCEDURES:

A copy of these procedures is included with the employee manual. These procedures are described in the training of all new staff and reinforced periodically to existing staff.

In the case of Natural Disaster or Fire:

-Staff should, as far as conditions allow:

1) Activate fire or tornado alarms manually, if they have not already been activated if applicable.

2) Notify the fire department (Phone 911). If the agency telephone system has been disrupted, utilize a staff member's personal cell phone.

For Staff located in the following counties:

- **BOONE STAFF** should, as far as conditions allow:

In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting in a safe location across the street from their building and meet on the SOUTH side of the building.

In the case of a tornado all employees will leave their office and go to the basement until an all clear is announced.

-**CERRO GORDO STAFF** should, as far as conditions allow:

In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building by the southwest stairwell out to the parking lot.

In the case of a tornado all employees will leave their office and go to the Conference Room across the hall until an all clear is announced.

-FRANKLIN STAFF should, as far as conditions allow**:**

In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting in a safe location across the street from their building.

In the case of a tornado all employees will leave their office and go to the basement until an all clear is announced.

-GREENE STAFF should as far as conditions allow:

In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting in a safe location by the Bell Tower.

In the case of a tornado all employees will leave their office and go to the basement until an all clear is announced.

-HAMILTON STAFF should as far as conditions allow:

In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting across the street on the South side of the building.

In the case of a tornado all employees will leave their office and go to the basement until an all clear is announced.

-HANCOCK STAFF-should as far as conditions allow:

In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at labeled exits and meeting in a safe location across the street from the building.

-HARDIN STAFF should as far as conditions allow**:**
In the case of fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting across the street on the South side of the Courthouse. If inclement weather staff should meet in the entryway of the Hardin County Sheriff's office.
In case of tornado, all employees will leave their offices and go to the basement until an all clear is announced.

-JASPER STAFF should as far as conditions allow:
In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting in a safe location across the street from their building.
In the case of a tornado all employees will leave their office and go to the basement until an all clear is announced.

-MADISON STAFF should as far as conditions allow:
In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting in a safe location across the street from their building and meet on the SOUTH side of the building.
In the case of a tornado all employees will leave their offices and go to the basement until an all clear is announced.

-MARSHALL STAFF should as far as conditions allow:
In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits.

-POWESHIEK STAFF should as far as conditions allow:
In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting in a safe location across the street from their building.
In the case of a tornado all employees will leave their office and go to the basement until an all clear is announced.

-STORY STAFF should as far as conditions allow:
In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building through the southeast door of HSC, unless blocked by fire. If blocked, use the northeast door or main entrance of HSC. Exit the building and meet across South Sherman Avenue to the east of the building in McDonald's parking lot.
In the case of a tornado all employees will leave their offices and go to the lower level of HSC in front of the CICS office until an all clear is announced.

-WARREN STAFF should as far as conditions allow:
In the case of a fire, all employees should immediately leave their offices, closing their doors behind them, exiting the building at the labeled exits and meet across the street on the East side of the building.
In case of a tornado all employees will leave their offices and go to the designated tornado shelter areas until an all clear is announced.

-WEBSTER STAFF should as far as conditions allow:
In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting in a safe location across the street from the building.
In the case of a tornado all employees will leave their office and go to the basement vault until an all clear is announced.

-WRIGHT STAFF should as far as conditions allow:
In the case of a fire, all employees should immediately leave their offices, ensuring that clients leave as well, closing their doors behind them, exiting the building at the labeled exits and meeting in a safe location across the street from their building and meet in Gazebo Park.
In the case of a tornado all employees will leave their office and go to the basement vault until an all clear is announced.

IX. Emergency Mode Operations.

If any Central Iowa Community Services offices become inoperable for a period of time, staff will work remotely. If necessary, staff will secure permission to operate from another County-owned office building on a temporary basis. If it appears that the Office will be inoperable for an extended period of time, we will operate out of another County.

In cases where access to buildings is not possible or advisable, such as during a pandemic, county staff shall work from home following HIPAA requirements as directed.

Document last updated: *4/1/2015, 6/1/2016, 7/1/2017, 6/21/2018, 5/6/2019, 6/1/2020, 6/29/21, 6/23/2022*

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is entered into by and between Franklin County, Iowa (the "Covered Entity"), and Central Iowa Community Services (the "Business Associate").

RECITALS

A. Covered Entity is a health care provider subject to the Health Insurance Portability and Accountability Act of 1996, the HITECH Act, and regulations promulgated thereunder ("HIPAA").

B. Business Associate, through the provision of certain services for or on behalf of the Covered Entity pursuant to a certain agreement entered into with Covered Entity effective on 7/1/22 for the provision by Business Associate of substance use disorder client funding eligibility and claim processing and administrative support services for Covered Entity (the "Services Agreement"), is a "business associate" of the Covered Entity as that term is defined in 45 C.F.R. § 160.103, and is subject to the Security Rule and certain provisions of the Privacy Rule.

C. Covered Entity is required by HIPAA to obtain satisfactory assurances that Business Associate will appropriately safeguard all PHI and Electronic PHI disclosed by, or created or received by Business Associate on behalf of, Covered Entity.

NOW, THEREFORE, in consideration of entering into the Services Agreement and the mutual promises and agreements below and in order to comply with all legal requirements, the parties agree as follows:

I. DEFINITIONS

1.1 **"Agreement"** has the meaning set forth in the preamble.

1.2 "**ARRA Breach**" has the same meaning as the term "Breach" in Section 13400(1) of the HITECH Act (i.e. 42 USCA 17921) and 45 CFR 164.402.

1.3 "**Business Associate**" has the meaning set forth in the preamble.

1.4 "**Covered Entity**" has the meaning set forth in the preamble.

1.5 "**Data Aggregation**" means the combining of PHI created or received under this Agreement with the PHI Business Associate receives or creates in its arrangement with another covered entity under the Privacy Rule to permit data analysis that relate to the Health Care Operations of the covered entities.

1.6 "**Designated Record Set**" means a group of records maintained by or for the Covered Entity that is: (i) the medical records and billing records about Individuals; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. As used herein the term "record" means any item, collection,

or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the Covered Entity.

1.7 "**Document Demand**" has the meaning set forth in Section 3.13.

1.8 "**Effective Date**" has the meaning set forth in the preamble.

1.9 "**Electronic PHI**" means information that comes within paragraphs 1(i) or 1(ii) of the definition of "PHI," as defined in 45 C.F.R. § 160.103, limited to the information created, received, maintained or transmitted by Business Associate on behalf of Covered Entity.

1.10 "**HIPAA**" has the meaning set forth in the Recitals.

1.11 "**HITECH Act**" means Title XIII and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law No. 111-5 and all regulations promulgated thereunder.

1.12 "**Individual**" means the person who is the subject of the PHI and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.13 "**PHI**" means Protected Health Information that is provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity.

1.14 "**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.

1.15 "**Protected Health Information**" (or "PHI") means any information, whether transmitted or maintained in electronic, written, oral, or any other form or medium, that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual; and (i) identifies the Individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

1.16 "**Required by Law**" has the same meaning as the term "'required by law" in 45 C.F.R. § 164.103.

1.17 "**Secretary**" means the Secretary of the U.S. Department of Health and Human Services or his or her designee.

1.18 "**Security Incident**" has the same meaning as the term "security incident" in 45 C.F.R. § 164.304.

1.19 "**Security Rule**" means the Security Standards and Implementation Specifications at 45 C.F.R. part 160 and part 164, subpart C.

1.20 "**Services Agreement**" has the meaning set forth in the Recitals.

1.21 "**Unsecured PHI**" or "**Unsecured PHI**" means PHI that is not secured through the use of a technology or methodology that the Secretary specifies in guidance renders PHI unusable, unreadable, or indecipherable to unauthorized Individuals, such as the guidance set forth in 74 Fed. Reg. 19006 (April 27, 2009) and updated in 74 Fed. Reg. 42740 (August 24, 2009).

1.22 Remaining Terms. Capitalized terms used, but not otherwise defined, in this Agreement have the meaning ascribed to them in HIPAA, the Privacy Rule, the Security Rule or the HITECH Act.

II. PERMITTED USES AND DISCLOSURES OF PHI

2.1 Services Agreement Uses and Disclosures. Business Associate may use or disclose PHI for purposes of performing its obligations and functions under the Services Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

2.2 Other Permitted Uses. If necessary, Business Associate may use PHI: (i) for the proper management and administration of the Business Associate; (ii) to carry out the legal responsibilities of the Business Associate; and (iii) for the provision of Data Aggregation services relating to the Health Care Operations of Covered Entity.

2.3 Other Permitted Disclosures. If necessary, Business Associate may disclose PHI for the purposes described in Section 2.2 above if: (i) the disclosure is Required by Law; or (ii) Business Associate obtains reasonable written assurance from the person or entity to whom it discloses the PHI that the PHI will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person or entity, and the person or entity notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

III. OBLIGATIONS OF BUSINESS ASSOCIATE

3.1 Compliance with Privacy Rule. Business Associate shall comply with all applicable provisions of the Privacy Rule in carrying out its obligations under the Services Agreement and this Agreement. Further, to the extent Business Associate is to carry out any of Covered Entity's obligations under subpart E of 45 CFR 164, Business Associate agrees to comply with the requirements of such subpart that apply to Covered Entity in the performance of such obligations.

3.2 Prohibition on Unauthorized Use or Disclosure. Business Associate shall not use or disclose PHI except as permitted by this Agreement or as Required by Law.

3.3 Minimum Necessary.

3.3.1 Business Associate shall limit its use and disclosure of PHI under this Agreement to the "minimum necessary," as set forth in guidance that the Secretary will issue regarding what constitutes "minimum necessary" under the Privacy Rule. Until the issuance of such guidance, Business Associate shall limit its use and disclosure of PHI, to the extent practicable, to the Limited Data Set (as that term is defined in 45 C.F.R.

§ 164.514(e)(2)), or, if needed, to the minimum necessary to accomplish the Business Associate's intended purpose. Business Associate may in good faith determine what constitutes the minimum necessary to accomplish the intended purpose of any disclosure of PHI.

3.3.2 Paragraph (a) above does not apply to: (1) disclosures to or requests by a health care provider for treatment; (2) uses or disclosures made to the Individual; (3) disclosures made pursuant to an authorization as set forth in 45 C.F.R. § 164.508; (4) disclosures made to the Secretary under 45 C.F.R. part 160, subpart C; (5) uses or disclosures that are Required by Law as described in 45 C.F.R. § 164.512(a); and (6) uses or disclosures that are required for compliance with applicable requirements of the Privacy Rule.

3.4 Safeguarding PHI; Security Regulations. Business Associate shall use appropriate administrative, physical, and technical safeguards and comply with the Security Rule with respect to Electronic PHI to prevent the use or disclosure of PHI other than as provided for by this Agreement.

3.5 Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Security Incident or a use or disclosure of PHI by Business Associate in violation of this Agreement.

3.6 Reporting. In the event that Business Associate becomes aware of a use or disclosure of PHI by Business Associate that is not permitted under this Agreement, Business Associate shall report such use or disclosure to the Covered Entity promptly in writing and in any event, within 5 days of becoming aware of the use or disclosure. Business Associate agrees to report to Covered Entity in writing any Security Incident of which it becomes aware, except that, for purposes of this reporting requirement the term "Security Incident" does not include inconsequential incidents that occur on a frequent basis such as scans or "pings" that are not allowed past Business Associate's firewall. Notwithstanding this Section 3.7, the Business Associate's reporting obligations regarding any ARRA Breach are set forth in Article IV.

3.7 Subcontractors. Business Associate shall ensure that all subcontractors or agents of Business Associate that create, receive, maintain or transmit PHI on behalf of the Business Associate agree in writing to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Business Associate shall ensure that all agents, including subcontractors, to whom it provides Electronic PHI, agree in writing to implement reasonable and appropriate safeguards to protect such Electronic PHI.

3.8 Access.

3.8.1 Within twenty (20) days of a request from Covered Entity, Business Associate shall furnish the PHI contained in a Designated Record Set that will enable the Covered Entity to respond to an Individual's request for inspection or copies of PHI about the Individual pursuant to 45 CFR § 164.524.

3.8.2 In the event an Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to the Covered Entity

immediately and take no direct immediate action on any such request. If the Covered Entity determines that an Individual is to be granted access to PHI, then Business Associate shall cooperate with the Covered Entity to provide to any Individual, at the Covered Entity's direction, any PHI requested by such Individual.

3.9 Amendment.

3.9.1 If the Covered Entity requests that Business Associate amend any Individual's PHI or a record regarding an Individual contained in a Designated Record Set, then Business Associate shall provide the relevant PHI to the Covered Entity for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526.

3.9.2 In the event an Individual requests directly to Business Associate that PHI be amended, Business Associate shall forward such request to the Covered Entity within ten (10) days of Business Associate's receipt of such request and shall take no direct immediate action on the request.

3.10 Records Availability. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining compliance with the Privacy Rule and the Security Rule.

3.11 Accounting of Disclosures.

3.11.1 If the Covered Entity requests that Business Associate furnish an accounting of disclosures of PHI made by Business Associate regarding an Individual during the six (6) years prior to the date on which the accounting was requested, then Business Associate shall, within fifteen (15) days of such request, make available to the Covered Entity such information as is in Business Associate's possession and is required for the Covered Entity to make the accounting required by 45 C.F.R. §164.528 and future regulations to be promulgated regarding accounting of disclosures.

3.11.2 In the event an Individual requests an accounting of disclosures directly from Business Associate, Business Associate shall within ten (10) days forward such request to the Covered Entity and shall take no direct action on the request.

3.12 Demands for Production of PHI.

3.12.1 Receipt by Business Associate. If Business Associate receives a subpoena, civil or administrative demand, or any other demand for production of PHI (a "Document Demand"), Business Associate shall provide a copy of such Document Demand to Covered Entity within five (5) days of receipt. To the extent the PHI that is the subject of the Document Demand is in the possession of Business Associate, and a response is warranted according to the standards contained in 45 C.F.R. § 164.512(e), Business Associate shall timely respond to the Document Demand.

3.12.2 Receipt by Covered Entity. If Covered Entity receives a Document Demand, Business Associate shall provide to Covered Entity any PHI responsive to such

Document Demand and assist and cooperate with Covered Entity in responding to such Document Demand in a timely manner and in accordance with the standards under 45 C.F.R. § 164.512(e).

3.13 Request for Restrictions on Disclosure of PHI. As required by Section 13405 of the HITECH Act and 45 CFR 164.522 (except as otherwise required by law), Business Associate shall comply with any request of an Individual for the Business Associate to restrict the disclosure of PHI of the Individual when the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment), and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

3.14 Remuneration for PHI.

3.14.1 Except as explicitly permitted in the Services Agreement and also set forth in paragraph (b) below, Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI of an Individual unless the Individual provided to the Covered Entity a valid authorization in accordance with 45 C.F.R. § 164.508 that specifically authorizes the Business Associate to exchange the PHI for remuneration.

3.14.2 Paragraph (a) above does not apply if the purpose of the exchange is: (1) for public health purposes pursuant to 45 CFR § 164.512(b) or § 164.514(e); (2) for research purposes pursuant to 45 CFR § 164.512(i) or § 164.514(e), where the only remuneration received by the Covered Entity or Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes; (3) for treatment and payment purposes pursuant to 45 CFR § 164.506(a); (4) for the sale, transfer, merger, or consolidation of all or part of the Covered Entity and for related due diligence as described in the HIPAA definition of health care operations and pursuant to 45 CFR § 164.506(a); (5) To or by a Business Associate for activities that the Business Associate undertakes on behalf of a Covered Entity (or on behalf of a Business Associate in the case of a subcontractor), pursuant to 45 CFR §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the Covered Entity to the Business Associate (or by the Business Associate to the subcontractor, if applicable), for the performance of such activities; (6) to an Individual, when the Individual requests access to his or her PHI pursuant to 45 CFR § 164.524 or when the Individual requests an accounting of disclosures pursuant to 45 CFR § 164.528; (7) for disclosures Required By Law; and (8) for any other purpose permitted by HIPAA where the only remuneration received by the Covered Entity or Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee expressly permitted by law.

3.15 Marketing Restrictions. Business associate shall ensure that any Marketing communications it makes on behalf of Covered Entity are in compliance with the rules governing marketing set forth in 45 C.F.R. 164.508(a)(3), including but not limited to the requirements that Business Associate must obtain an authorization from an Individual prior to making any marketing communication to such Individual.

3.16 Fundraising Limitations. Business Associate shall ensure that any fundraising communications Business Associate makes on behalf of the Covered Entity are in compliance with the rules governing fundraising communications set forth in 45 C.F.R. 164.514(f), including but not limited to the requirement that Business Associate must provide, with each fundraising communication made to an Individual, a clear and conspicuous opportunity for the recipient of the communication to elect not to receive any further fundraising communications. Business Associate shall ensure that all Individuals electing not to receive any further fundraising communications do not receive any further fundraising communications.

IV. ARRA BREACH NOTIFICATION.

4.1 Risk Assessment by Business Associate. If Business Associate becomes aware of a potential ARRA Breach, Business Associate shall complete a risk assessment of the potential ARRA Breach to determine whether the potential ARRA Breach is an ARRA Breach. Such risk assessment shall include at least all the factors identified in 45 CFR 164.402(2), as amended by the final rule published in the Federal Register on January 25, 2013 at 78 Fed. Reg. 5566.

4.2 Notification to Covered Entity. If, after completing such risk assessment, Business Associate concludes that there was an ARRA Breach, Business Associate shall notify the Covered Entity of the ARRA Breach as soon as reasonably possible, and in all cases within five (5) business days of the first day on which any employee, officer or agent of Business Associate either knows or by exercising reasonable diligence would have known that an ARRA Breach occurred. The notification to Covered Entity shall include, if known, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed during such ARRA Breach. The notification shall also include: (a) a brief description of what happened, including the date of the ARRA Breach and the date of the discovery of the ARRA Breach, if known; (b) a description of the types of Unsecured PHI that were involved in the ARRA Breach (such as whether the full name, social security number, date of birth, home address, account number, diagnosis disability code or other types of information were involved); (c) recommended steps that Individuals should take to protect themselves from potential harm resulting from the ARRA Breach; and (d) a brief description of what the Business Associate is doing to investigate the ARRA Breach, to mitigate harm to Individuals, and to protect against any further ARRA Breaches. Business Associate shall maintain evidence to demonstrate that any required risk assessment was completed and notification to the Covered Entity under this paragraph was made unless the Business Associate determines that a delayed notice (as described in Section 4.3) applies.

4.3 Delayed Notification to Covered Entity. Notwithstanding Section 4.2 above, if a law enforcement official states in writing to Business Associate that the notification to Covered Entity required under Section 4.2 would impede a criminal investigation or cause damage to national security, then Business Associate may delay the notification for any period of time set forth in the written statement of the law enforcement official. If the law enforcement official provides an oral statement, then Business Associate shall document the statement in writing, including the name of the law enforcement official making the statement, and may delay the notification required under Section 4.2 for no longer than thirty (30) days from the date of the oral statement, unless the law enforcement official provides a written statement during that time that specifies a different time period. Business Associate shall be obligated to maintain evidence to

demonstrate the reason for the delayed notification and that the required notification under this paragraph was made

4.4 Notification to Individuals, the Secretary and/or the Media. In the event of an ARRA Breach caused by Business Associate, its agents and/or subcontractors, Business Associate shall provide assistance to Covered Entity in making all ARRA Breach notifications. To the extent Covered Entity incurs expenses and costs to comply with its notification obligations with respect to an ARRA Breach by Business Associate, its agents and/or subcontractors, in addition to any other remedies that may be available to Covered Entity under this Agreement or any applicable law, Business Associate shall reimburse Covered Entity for all costs and expenses (including attorneys' fees) incurred by Covered Entity related to providing the notifications required under 45 C.F.R. §§ 164.404, 406 and 408. Notwithstanding the foregoing, if the parties agree that Business Associate will, on behalf of Covered Entity, and within the applicable time frames required by law under 45 C.F.R. §§ 164.404, 406 and 408, prepare and send out any and all required ARRA Breach notifications to Individuals, the Secretary and/or to the media, Business Associate shall prepare and send such ARRA Breach notifications at Business Associate's sole expense and in compliance with the requirements of 45 C.F.R. 164.404, 406 and 408, as applicable. However, any ARRA Breach notifications Business Associate would prepare and send on behalf of Covered Entity shall be subject to Covered Entity's review and pre-approval before the notifications are sent. Additionally, in the event of an ARRA Breach, Business Associate agrees to pay for the credit monitoring fees for affected Individuals for a period of at least two (2) years of credit monitoring.

V. TERM AND TERMINATION

5.1 Term. This Agreement is effective upon the effective date of the Services Agreement, and except for the rights and obligations set forth in this Agreement specifically surviving termination, shall terminate the later of the date the Services Agreement terminates or when all PHI is returned to Covered Entity or, with prior permission of Covered Entity, destroyed.

5.2 Termination for Cause. Notwithstanding any provision in this Agreement, Covered Entity may terminate this Agreement and the Services Agreement if Covered Entity determines, in its sole discretion, Business Associate has breached any provision of this Agreement or otherwise violated HIPAA, the Privacy Rule, the Security Rule or the HITECH Act. Covered Entity shall provide written notice to Business Associate with an opportunity for Business Associate to cure the breach or end the violation within ten (10) business days of such written notice, unless cure is not possible. If Business Associate fails to cure the breach or end the violation within the specified time period, or if cure is not possible, this Agreement and the Service Agreement shall automatically and immediately terminate, unless termination is infeasible.

5.3 Termination after Repeated Violations. Notwithstanding any provision in the Agreement, Covered Entity may terminate the Services Agreement and this Agreement if Covered Entity determines, in its sole discretion, that Business Associate has repeatedly breached any provision of this Agreement or otherwise violated HIPAA, the Privacy Rule, the Security Rule or the HITECH Act, irrespective of whether, or how promptly, Business Associate may remedy such violation after being notified of the same.

5.4 Obligations Upon Termination. Business Associate's obligations to protect the privacy and security of PHI shall be continuous and shall survive termination, cancellation, expiration or other conclusion of this Agreement or the Services Agreement. Upon termination of this Agreement, Business Associate will forward to Covered Entity, or to Covered Entity's designee, the records necessary for continued administration of Covered Entity as directed by Covered Entity. After the forwarding of said records, whatever PHI remains with Business Associate will be subject to the following:

5.4.1 Except as provided in paragraph (b) of this Section 5.4, upon termination, cancellation, expiration or other conclusion of this Agreement, for any reason, Business Associate shall return or, if Covered Entity gives written permission, destroy, PHI in whatever form or medium and retain no copies of such PHI. Business Associate will complete such return or destruction as soon as possible, but in no event later than sixty (60) days from the date of the termination of this Agreement. Within ten (10) days of the return or destruction of all PHI by Business Associate, Business Associate shall provide written certification to Covered Entity that the return or destruction of PHI has been completed.

5.4.2 In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VI. INDEMNIFICATION; INSURANCE

6.1 Indemnification by Business Associate. Business Associate will indemnify and hold harmless Covered Entity, and any affiliate, officer, director, employee or agent of Covered Entity from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any use or disclosure of PHI that violates or is not permitted by this Agreement, HIPAA, the Privacy Rule, the Security Rule or the HITECH Act, or other breach of this Agreement by Business Associate or any subcontractor or agent of Business Associate.

6.2 Right to Tender or Undertake Defense. If Covered Entity is named as a party in any judicial, administrative or other proceeding arising out of or in connection with any non-permitted or violating use or disclosure of PHI or other breach of this Agreement by Business Associate or any subcontractor or agent of Business Associate, Covered Entity shall have the option at any time either to: (i) tender its defense to Business Associate, in which case Business Associate will provide qualified attorneys, consultants, and other appropriate professionals to represent Covered Entity's interests at Business Associate's expense; or (ii) undertake its own defense, choosing the attorneys, consultants, and other appropriate professionals to represent its interests, in which case Business Associate will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants, and other professionals.

6.3 Right to Control Resolution. Covered Entity has the sole right and discretion to settle, compromise or otherwise resolve any and all claims, causes of actions, liabilities or damages against it, notwithstanding that Covered Entity may have tendered its defense to Business Associate. Any such resolution will not relieve Business Associate of its obligation to indemnify Covered Entity under this Agreement.

6.4 Insurance. Upon request, Business Associate shall obtain and maintain insurance coverage against improper uses and disclosures of PHI by Business Associate, naming Covered Entity as an additional named insured. Upon request, Business Associate shall provide a certificate evidencing such insurance coverage.

6.5 Conflicts. With respect to any breaches or violations of this Agreement, the provisions in this Section 6 supersede any inconsistent terms contained in the Services Agreement.

VII. GENERAL PROVISIONS

7.1 Effect. The terms and provisions of this Agreement supersede any other conflicting or inconsistent terms and provisions in any agreements between the parties, including all exhibits or other attachments thereto and all documents incorporated therein by reference.

7.2 Amendment. Business Associate and the Covered Entity agree to amend this Agreement to the extent necessary to allow either party to comply with HIPAA, the Privacy Rule, the Security Rule, or the HITECH Act. All such amendments shall be made in a writing signed by both parties.

7.3 No Third Party Beneficiaries. This Agreement is intended for the benefit of Business Associate and Covered Entity only. Nothing express or implied is intended to confer or create, nor be interpreted to confer or create, any rights, remedies, obligations or liabilities to or for any third party beneficiary, including without limitation Individuals who are the subject of PHI.

7.4 Severability. In the event that any provision of this Agreement violates any applicable statute, ordinance, or rule of law in any jurisdiction that governs this Agreement, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this Agreement.

7.5 No Waiver. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.

7.6 Assignment. This Agreement may not be assigned by either party without the prior written consent of the other party; provided, however, that the parties shall cooperate to assign this Agreement as appropriate if the Services Agreement is assigned.

7.7 Relationship of the Parties. Business Associate and Covered Entity are independent contractors and all acts performed by Business Associate are performed solely in its capacity as an independent contractor.

7.8 Counterparts; Facsimile Signature. This Agreement may be executed by facsimile and/or in counterparts, each of which shall be an original and all of which together shall constitute one and the same binding instrument.

7.9 Notification

7.9.1 Business Associate. To the extent notice is required to be provided by Covered Entity to Business Associate under any provision in this Agreement, notice shall be provided to:

Russell Wood
russell.wood@cicsmhds.org
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010
Phone 515-663-2928

7.9.2 Covered Entity. To the extent notice is required to be provided by Business Associate to Covered Entity under any provision in this Agreement, notice shall be provided to:

Katy Flint
KFlint@co.franklin.ia.us
12 1st Ave NW
Hampton, IA 50441
641-456-5622

7.10 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA, the Privacy Rule, the Security Rule, and the HITECH Act.

INTENDING TO BE LEGALLY BOUND, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

BUSINESS ASSOCIATE

Central Iowa Community Services

By: _____

Print Name: _____

Title: _____

Date: _____

COVERED ENTITY

Franklin County, Iowa

By: Gary McVicker

Print Name: Gary McVicker

Title: Board Chairman

Date: 12/20/22

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is entered into by and between __Hardin County__, Iowa (the "Covered Entity"), and Central Iowa Community Services (the "Business Associate").

RECITALS

A. Covered Entity is a health care provider subject to the Health Insurance Portability and Accountability Act of 1996, the HITECH Act, and regulations promulgated thereunder ("HIPAA").

B. Business Associate, through the provision of certain services for or on behalf of the Covered Entity pursuant to a certain agreement entered into with Covered Entity effective on 7/1/22 for the provision by Business Associate of substance use disorder client funding eligibility and claim processing for Covered Entity (the "Services Agreement"), is a "business associate" of the Covered Entity as that term is defined in 45 C.F.R. § 160.103, and is subject to the Security Rule and certain provisions of the Privacy Rule.

C. Covered Entity is required by HIPAA to obtain satisfactory assurances that Business Associate will appropriately safeguard all PHI and Electronic PHI disclosed by, or created or received by Business Associate on behalf of, Covered Entity.

NOW, THEREFORE, in consideration of entering into the Services Agreement and the mutual promises and agreements below and in order to comply with all legal requirements, the parties agree as follows:

I. DEFINITIONS

1.1 "Agreement" has the meaning set forth in the preamble.

1.2 "**ARRA Breach**" has the same meaning as the term "Breach" in Section 13400(1) of the HITECH Act (i.e. 42 USCA 17921) and 45 CFR 164.402.

1.3 "**Business Associate**" has the meaning set forth in the preamble.

1.4 "**Covered Entity**" has the meaning set forth in the preamble.

1.5 "**Data Aggregation**" means the combining of PHI created or received under this Agreement with the PHI Business Associate receives or creates in its arrangement with another covered entity under the Privacy Rule to permit data analysis that relate to the Health Care Operations of the covered entities.

1.6 "**Designated Record Set**" means a group of records maintained by or for the Covered Entity that is: (i) the medical records and billing records about Individuals; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. As used herein the term "record" means any item, collection,

or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the Covered Entity.

1.7 "**Document Demand**" has the meaning set forth in Section 3.13.

1.8 "**Effective Date**" has the meaning set forth in the preamble.

1.9 "**Electronic PHI**" means information that comes within paragraphs 1(i) or 1(ii) of the definition of "PHI," as defined in 45 C.F.R. § 160.103, limited to the information created, received, maintained or transmitted by Business Associate on behalf of Covered Entity.

1.10 "**HIPAA**" has the meaning set forth in the Recitals.

1.11 "**HITECH Act**" means Title XIII and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law No. 111-5 and all regulations promulgated thereunder.

1.12 "**Individual**" means the person who is the subject of the PHI and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.13 "**PHI**" means Protected Health Information that is provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity.

1.14 "**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.

1.15 "**Protected Health Information**" (or "PHI") means any information, whether transmitted or maintained in electronic, written, oral, or any other form or medium, that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual; and (i) identifies the Individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

1.16 "**Required by Law**" has the same meaning as the term "'required by law" in 45 C.F.R. § 164.103.

1.17 "**Secretary**" means the Secretary of the U.S. Department of Health and Human Services or his or her designee.

1.18 "**Security Incident**" has the same meaning as the term "security incident" in 45 C.F.R. § 164.304.

1.19 "**Security Rule**" means the Security Standards and Implementation Specifications at 45 C.F.R. part 160 and part 164, subpart C.

1.20 "**Services Agreement**" has the meaning set forth in the Recitals.

1.21 "**Unsecured PHI**" or "**Unsecured PHI**" means PHI that is not secured through the use of a technology or methodology that the Secretary specifies in guidance renders PHI unusable, unreadable, or indecipherable to unauthorized Individuals, such as the guidance set forth in 74 Fed. Reg. 19006 (April 27, 2009) and updated in 74 Fed. Reg. 42740 (August 24, 2009).

1.22 Remaining Terms. Capitalized terms used, but not otherwise defined, in this Agreement have the meaning ascribed to them in HIPAA, the Privacy Rule, the Security Rule or the HITECH Act.

II. PERMITTED USES AND DISCLOSURES OF PHI

2.1 Services Agreement Uses and Disclosures. Business Associate may use or disclose PHI for purposes of performing its obligations and functions under the Services Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

2.2 Other Permitted Uses. If necessary, Business Associate may use PHI: (i) for the proper management and administration of the Business Associate; (ii) to carry out the legal responsibilities of the Business Associate; and (iii) for the provision of Data Aggregation services relating to the Health Care Operations of Covered Entity.

2.3 Other Permitted Disclosures. If necessary, Business Associate may disclose PHI for the purposes described in Section 2.2 above if: (i) the disclosure is Required by Law; or (ii) Business Associate obtains reasonable written assurance from the person or entity to whom it discloses the PHI that the PHI will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person or entity, and the person or entity notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

III. OBLIGATIONS OF BUSINESS ASSOCIATE

3.1 Compliance with Privacy Rule. Business Associate shall comply with all applicable provisions of the Privacy Rule in carrying out its obligations under the Services Agreement and this Agreement. Further, to the extent Business Associate is to carry out any of Covered Entity's obligations under subpart E of 45 CFR 164, Business Associate agrees to comply with the requirements of such subpart that apply to Covered Entity in the performance of such obligations.

3.2 Prohibition on Unauthorized Use or Disclosure. Business Associate shall not use or disclose PHI except as permitted by this Agreement or as Required by Law.

3.3 Minimum Necessary.

3.3.1 Business Associate shall limit its use and disclosure of PHI under this Agreement to the "minimum necessary," as set forth in guidance that the Secretary will issue regarding what constitutes "minimum necessary" under the Privacy Rule. Until the issuance of such guidance, Business Associate shall limit its use and disclosure of PHI, to the extent practicable, to the Limited Data Set (as that term is defined in 45 C.F.R.

§ 164.514(e)(2)), or, if needed, to the minimum necessary to accomplish the Business Associate's intended purpose. Business Associate may in good faith determine what constitutes the minimum necessary to accomplish the intended purpose of any disclosure of PHI.

3.3.2 Paragraph (a) above does not apply to: (1) disclosures to or requests by a health care provider for treatment; (2) uses or disclosures made to the Individual; (3) disclosures made pursuant to an authorization as set forth in 45 C.F.R. § 164.508; (4) disclosures made to the Secretary under 45 C.F.R. part 160, subpart C; (5) uses or disclosures that are Required by Law as described in 45 C.F.R. § 164.512(a); and (6) uses or disclosures that are required for compliance with applicable requirements of the Privacy Rule.

3.4 Safeguarding PHI; Security Regulations. Business Associate shall use appropriate administrative, physical, and technical safeguards and comply with the Security Rule with respect to Electronic PHI to prevent the use or disclosure of PHI other than as provided for by this Agreement.

3.5 Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Security Incident or a use or disclosure of PHI by Business Associate in violation of this Agreement.

3.6 Reporting. In the event that Business Associate becomes aware of a use or disclosure of PHI by Business Associate that is not permitted under this Agreement, Business Associate shall report such use or disclosure to the Covered Entity promptly in writing and in any event, within 5 days of becoming aware of the use or disclosure. Business Associate agrees to report to Covered Entity in writing any Security Incident of which it becomes aware, except that, for purposes of this reporting requirement the term "Security Incident" does not include inconsequential incidents that occur on a frequent basis such as scans or "pings" that are not allowed past Business Associate's firewall. Notwithstanding this Section 3.7, the Business Associate's reporting obligations regarding any ARRA Breach are set forth in Article IV.

3.7 Subcontractors. Business Associate shall ensure that all subcontractors or agents of Business Associate that create, receive, maintain or transmit PHI on behalf of the Business Associate agree in writing to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Business Associate shall ensure that all agents, including subcontractors, to whom it provides Electronic PHI, agree in writing to implement reasonable and appropriate safeguards to protect such Electronic PHI.

3.8 Access.

3.8.1 Within twenty (20) days of a request from Covered Entity, Business Associate shall furnish the PHI contained in a Designated Record Set that will enable the Covered Entity to respond to an Individual's request for inspection or copies of PHI about the Individual pursuant to 45 CFR § 164.524.

3.8.2 In the event an Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to the Covered Entity

immediately and take no direct immediate action on any such request. If the Covered Entity determines that an Individual is to be granted access to PHI, then Business Associate shall cooperate with the Covered Entity to provide to any Individual, at the Covered Entity's direction, any PHI requested by such Individual.

3.9 Amendment.

3.9.1 If the Covered Entity requests that Business Associate amend any Individual's PHI or a record regarding an Individual contained in a Designated Record Set, then Business Associate shall provide the relevant PHI to the Covered Entity for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526.

3.9.2 In the event an Individual requests directly to Business Associate that PHI be amended, Business Associate shall forward such request to the Covered Entity within ten (10) days of Business Associate's receipt of such request and shall take no direct immediate action on the request.

3.10 Records Availability. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining compliance with the Privacy Rule and the Security Rule.

3.11 Accounting of Disclosures.

3.11.1 If the Covered Entity requests that Business Associate furnish an accounting of disclosures of PHI made by Business Associate regarding an Individual during the six (6) years prior to the date on which the accounting was requested, then Business Associate shall, within fifteen (15) days of such request, make available to the Covered Entity such information as is in Business Associate's possession and is required for the Covered Entity to make the accounting required by 45 C.F.R. §164.528 and future regulations to be promulgated regarding accounting of disclosures.

3.11.2 In the event an Individual requests an accounting of disclosures directly from Business Associate, Business Associate shall within ten (10) days forward such request to the Covered Entity and shall take no direct action on the request.

3.12 Demands for Production of PHI.

3.12.1 Receipt by Business Associate. If Business Associate receives a subpoena, civil or administrative demand, or any other demand for production of PHI (a "Document Demand"), Business Associate shall provide a copy of such Document Demand to Covered Entity within five (5) days of receipt. To the extent the PHI that is the subject of the Document Demand is in the possession of Business Associate, and a response is warranted according to the standards contained in 45 C.F.R. § 164.512(e), Business Associate shall timely respond to the Document Demand.

3.12.2 Receipt by Covered Entity. If Covered Entity receives a Document Demand, Business Associate shall provide to Covered Entity any PHI responsive to such

Document Demand and assist and cooperate with Covered Entity in responding to such Document Demand in a timely manner and in accordance with the standards under 45 C.F.R. § 164.512(e).

3.13 Request for Restrictions on Disclosure of PHI. As required by Section 13405 of the HITECH Act and 45 CFR 164.522 (except as otherwise required by law), Business Associate shall comply with any request of an Individual for the Business Associate to restrict the disclosure of PHI of the Individual when the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment), and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

3.14 Remuneration for PHI.

3.14.1 Except as explicitly permitted in the Services Agreement and also set forth in paragraph (b) below, Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI of an Individual unless the Individual provided to the Covered Entity a valid authorization in accordance with 45 C.F.R. § 164.508 that specifically authorizes the Business Associate to exchange the PHI for remuneration.

3.14.2 Paragraph (a) above does not apply if the purpose of the exchange is: (1) for public health purposes pursuant to 45 CFR § 164.512(b) or § 164.514(e); (2) for research purposes pursuant to 45 CFR § 164.512(i) or § 164.514(e), where the only remuneration received by the Covered Entity or Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes; (3) for treatment and payment purposes pursuant to 45 CFR § 164.506(a); (4) for the sale, transfer, merger, or consolidation of all or part of the Covered Entity and for related due diligence as described in the HIPAA definition of health care operations and pursuant to 45 CFR § 164.506(a); (5) To or by a Business Associate for activities that the Business Associate undertakes on behalf of a Covered Entity (or on behalf of a Business Associate in the case of a subcontractor), pursuant to 45 CFR §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the Covered Entity to the Business Associate (or by the Business Associate to the subcontractor, if applicable), for the performance of such activities; (6) to an Individual, when the Individual requests access to his or her PHI pursuant to 45 CFR § 164.524 or when the Individual requests an accounting of disclosures pursuant to 45 CFR § 164.528; (7) for disclosures Required By Law; and (8) for any other purpose permitted by HIPAA where the only remuneration received by the Covered Entity or Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee expressly permitted by law.

3.15 Marketing Restrictions. Business associate shall ensure that any Marketing communications it makes on behalf of Covered Entity are in compliance with the rules governing marketing set forth in 45 C.F.R. 164.508(a)(3), including but not limited to the requirements that Business Associate must obtain an authorization from an Individual prior to making any marketing communication to such Individual.

3.16 Fundraising Limitations. Business Associate shall ensure that any fundraising communications Business Associate makes on behalf of the Covered Entity are in compliance with the rules governing fundraising communications set forth in 45 C.F.R. 164.514(f), including but not limited to the requirement that Business Associate must provide, with each fundraising communication made to an Individual, a clear and conspicuous opportunity for the recipient of the communication to elect not to receive any further fundraising communications. Business Associate shall ensure that all Individuals electing not to receive any further fundraising communications do not receive any further fundraising communications.

IV. ARRA BREACH NOTIFICATION.

4.1 Risk Assessment by Business Associate. If Business Associate becomes aware of a potential ARRA Breach, Business Associate shall complete a risk assessment of the potential ARRA Breach to determine whether the potential ARRA Breach is an ARRA Breach. Such risk assessment shall include at least all the factors identified in 45 CFR 164.402(2), as amended by the final rule published in the Federal Register on January 25, 2013 at 78 Fed. Reg. 5566.

4.2 Notification to Covered Entity. If, after completing such risk assessment, Business Associate concludes that there was an ARRA Breach, Business Associate shall notify the Covered Entity of the ARRA Breach as soon as reasonably possible, and in all cases within five (5) business days of the first day on which any employee, officer or agent of Business Associate either knows or by exercising reasonable diligence would have known that an ARRA Breach occurred. The notification to Covered Entity shall include, if known, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed during such ARRA Breach. The notification shall also include: (a) a brief description of what happened, including the date of the ARRA Breach and the date of the discovery of the ARRA Breach, if known; (b) a description of the types of Unsecured PHI that were involved in the ARRA Breach (such as whether the full name, social security number, date of birth, home address, account number, diagnosis disability code or other types of information were involved); (c) recommended steps that Individuals should take to protect themselves from potential harm resulting from the ARRA Breach; and (d) a brief description of what the Business Associate is doing to investigate the ARRA Breach, to mitigate harm to Individuals, and to protect against any further ARRA Breaches. Business Associate shall maintain evidence to demonstrate that any required risk assessment was completed and notification to the Covered Entity under this paragraph was made unless the Business Associate determines that a delayed notice (as described in Section 4.3) applies.

4.3 Delayed Notification to Covered Entity. Notwithstanding Section 4.2 above, if a law enforcement official states in writing to Business Associate that the notification to Covered Entity required under Section 4.2 would impede a criminal investigation or cause damage to national security, then Business Associate may delay the notification for any period of time set forth in the written statement of the law enforcement official. If the law enforcement official provides an oral statement, then Business Associate shall document the statement in writing, including the name of the law enforcement official making the statement, and may delay the notification required under Section 4.2 for no longer than thirty (30) days from the date of the oral statement, unless the law enforcement official provides a written statement during that time that specifies a different time period. Business Associate shall be obligated to maintain evidence to

demonstrate the reason for the delayed notification and that the required notification under this paragraph was made

4.4 Notification to Individuals, the Secretary and/or the Media. In the event of an ARRA Breach caused by Business Associate, its agents and/or subcontractors, Business Associate shall provide assistance to Covered Entity in making all ARRA Breach notifications. To the extent Covered Entity incurs expenses and costs to comply with its notification obligations with respect to an ARRA Breach by Business Associate, its agents and/or subcontractors, in addition to any other remedies that may be available to Covered Entity under this Agreement or any applicable law, Business Associate shall reimburse Covered Entity for all costs and expenses (including attorneys' fees) incurred by Covered Entity related to providing the notifications required under 45 C.F.R. §§ 164.404, 406 and 408. Notwithstanding the foregoing, if the parties agree that Business Associate will, on behalf of Covered Entity, and within the applicable time frames required by law under 45 C.F.R. §§ 164.404, 406 and 408, prepare and send out any and all required ARRA Breach notifications to Individuals, the Secretary and/or to the media, Business Associate shall prepare and send such ARRA Breach notifications at Business Associate's sole expense and in compliance with the requirements of 45 C.F.R. 164.404, 406 and 408, as applicable. However, any ARRA Breach notifications Business Associate would prepare and send on behalf of Covered Entity shall be subject to Covered Entity's review and pre-approval before the notifications are sent. Additionally, in the event of an ARRA Breach, Business Associate agrees to pay for the credit monitoring fees for affected Individuals for a period of at least two (2) years of credit monitoring.

V. TERM AND TERMINATION

5.1 Term. This Agreement is effective upon the effective date of the Services Agreement, and except for the rights and obligations set forth in this Agreement specifically surviving termination, shall terminate the later of the date the Services Agreement terminates or when all PHI is returned to Covered Entity or, with prior permission of Covered Entity, destroyed.

5.2 Termination for Cause. Notwithstanding any provision in this Agreement, Covered Entity may terminate this Agreement and the Services Agreement if Covered Entity determines, in its sole discretion, Business Associate has breached any provision of this Agreement or otherwise violated HIPAA, the Privacy Rule, the Security Rule or the HITECH Act. Covered Entity shall provide written notice to Business Associate with an opportunity for Business Associate to cure the breach or end the violation within ten (10) business days of such written notice, unless cure is not possible. If Business Associate fails to cure the breach or end the violation within the specified time period, or if cure is not possible, this Agreement and the Service Agreement shall automatically and immediately terminate, unless termination is infeasible.

5.3 Termination after Repeated Violations. Notwithstanding any provision in the Agreement, Covered Entity may terminate the Services Agreement and this Agreement if Covered Entity determines, in its sole discretion, that Business Associate has repeatedly breached any provision of this Agreement or otherwise violated HIPAA, the Privacy Rule, the Security Rule or the HITECH Act, irrespective of whether, or how promptly, Business Associate may remedy such violation after being notified of the same.

5.4 Obligations Upon Termination. Business Associate's obligations to protect the privacy and security of PHI shall be continuous and shall survive termination, cancellation, expiration or other conclusion of this Agreement or the Services Agreement. Upon termination of this Agreement, Business Associate will forward to Covered Entity, or to Covered Entity's designee, the records necessary for continued administration of Covered Entity as directed by Covered Entity. After the forwarding of said records, whatever PHI remains with Business Associate will be subject to the following:

5.4.1 Except as provided in paragraph (b) of this Section 5.4, upon termination, cancellation, expiration or other conclusion of this Agreement, for any reason, Business Associate shall return or, if Covered Entity gives written permission, destroy, PHI in whatever form or medium and retain no copies of such PHI. Business Associate will complete such return or destruction as soon as possible, but in no event later than sixty (60) days from the date of the termination of this Agreement. Within ten (10) days of the return or destruction of all PHI by Business Associate, Business Associate shall provide written certification to Covered Entity that the return or destruction of PHI has been completed.

5.4.2 In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VI. INDEMNIFICATION; INSURANCE

6.1 Indemnification by Business Associate. Business Associate will indemnify and hold harmless Covered Entity, and any affiliate, officer, director, employee or agent of Covered Entity from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any use or disclosure of PHI that violates or is not permitted by this Agreement, HIPAA, the Privacy Rule, the Security Rule or the HITECH Act, or other breach of this Agreement by Business Associate or any subcontractor or agent of Business Associate.

6.2 Right to Tender or Undertake Defense. If Covered Entity is named as a party in any judicial, administrative or other proceeding arising out of or in connection with any non-permitted or violating use or disclosure of PHI or other breach of this Agreement by Business Associate or any subcontractor or agent of Business Associate, Covered Entity shall have the option at any time either to: (i) tender its defense to Business Associate, in which case Business Associate will provide qualified attorneys, consultants, and other appropriate professionals to represent Covered Entity's interests at Business Associate's expense; or (ii) undertake its own defense, choosing the attorneys, consultants, and other appropriate professionals to represent its interests, in which case Business Associate will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants, and other professionals.

6.3 Right to Control Resolution. Covered Entity has the sole right and discretion to settle, compromise or otherwise resolve any and all claims, causes of actions, liabilities or damages against it, notwithstanding that Covered Entity may have tendered its defense to Business Associate. Any such resolution will not relieve Business Associate of its obligation to indemnify Covered Entity under this Agreement.

6.4 Insurance. Upon request, Business Associate shall obtain and maintain insurance coverage against improper uses and disclosures of PHI by Business Associate, naming Covered Entity as an additional named insured. Upon request, Business Associate shall provide a certificate evidencing such insurance coverage.

6.5 Conflicts. With respect to any breaches or violations of this Agreement, the provisions in this Section 6 supersede any inconsistent terms contained in the Services Agreement.

VII. GENERAL PROVISIONS

7.1 Effect. The terms and provisions of this Agreement supersede any other conflicting or inconsistent terms and provisions in any agreements between the parties, including all exhibits or other attachments thereto and all documents incorporated therein by reference.

7.2 Amendment. Business Associate and the Covered Entity agree to amend this Agreement to the extent necessary to allow either party to comply with HIPAA, the Privacy Rule, the Security Rule, or the HITECH Act. All such amendments shall be made in a writing signed by both parties.

7.3 No Third Party Beneficiaries. This Agreement is intended for the benefit of Business Associate and Covered Entity only. Nothing express or implied is intended to confer or create, nor be interpreted to confer or create, any rights, remedies, obligations or liabilities to or for any third party beneficiary, including without limitation Individuals who are the subject of PHI.

7.4 Severability. In the event that any provision of this Agreement violates any applicable statute, ordinance, or rule of law in any jurisdiction that governs this Agreement, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this Agreement.

7.5 No Waiver. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.

7.6 Assignment. This Agreement may not be assigned by either party without the prior written consent of the other party; provided, however, that the parties shall cooperate to assign this Agreement as appropriate if the Services Agreement is assigned.

7.7 Relationship of the Parties. Business Associate and Covered Entity are independent contractors and all acts performed by Business Associate are performed solely in its capacity as an independent contractor.

7.8 Counterparts; Facsimile Signature. This Agreement may be executed by facsimile and/or in counterparts, each of which shall be an original and all of which together shall constitute one and the same binding instrument.

7.9 Notification

7.9.1 Business Associate. To the extent notice is required to be provided by Covered Entity to Business Associate under any provision in this Agreement, notice shall be provided to:

Russell Wood
russell.wood@cicsmhds.org
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010
Phone 515-663-2928

7.9.2 Covered Entity. To the extent notice is required to be provided by Business Associate to Covered Entity under any provision in this Agreement, notice shall be provided to:

Jolene Pieters
jpieters@hardincountyia.gov
1215 Edgington Avenue, Suite 1
Eldora, IA 50627
Phone: 641-939-8108
Fax: 641-939-8223

7.10 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA, the Privacy Rule, the Security Rule, and the HITECH Act.

INTENDING TO BE LEGALLY BOUND, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

BUSINESS ASSOCIATE

Franklin County, Iowa

By: _____

Print Name: _____

Title: _____

Date: _____

COVERED ENTITY

Hardin County, Iowa

By: _____

Print Name: BJ Hoffman

Title: Chairman

Date: 6/21/22

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is entered into by and between Story County, Iowa (the "Covered Entity"), and Central Iowa Community Services (the "Business Associate").

RECITALS

A. Covered Entity is a health care provider subject to the Health Insurance Portability and Accountability Act of 1996, the HITECH Act, and regulations promulgated thereunder ("HIPAA").

B. Business Associate, through the provision of certain services for or on behalf of the Covered Entity pursuant to a certain agreement entered into with Covered Entity effective on 7/1/22 for the provision by Business Associate of substance use disorder client funding eligibility and claim processing and administrative support services for Covered Entity (the "Services Agreement"), is a "business associate" of the Covered Entity as that term is defined in 45 C.F.R. § 160.103, and is subject to the Security Rule and certain provisions of the Privacy Rule.

C. Covered Entity is required by HIPAA to obtain satisfactory assurances that Business Associate will appropriately safeguard all PHI and Electronic PHI disclosed by, or created or received by Business Associate on behalf of, Covered Entity.

NOW, THEREFORE, in consideration of entering into the Services Agreement and the mutual promises and agreements below and in order to comply with all legal requirements, the parties agree as follows:

I. DEFINITIONS

1.1 **"Agreement"** has the meaning set forth in the preamble.

1.2 "**ARRA Breach**" has the same meaning as the term "Breach" in Section 13400(1) of the HITECH Act (i.e. 42 USCA 17921) and 45 CFR 164.402.

1.3 "**Business Associate**" has the meaning set forth in the preamble.

1.4 "**Covered Entity**" has the meaning set forth in the preamble.

1.5 "**Data Aggregation**" means the combining of PHI created or received under this Agreement with the PHI Business Associate receives or creates in its arrangement with another covered entity under the Privacy Rule to permit data analysis that relate to the Health Care Operations of the covered entities.

1.6 "**Designated Record Set**" means a group of records maintained by or for the Covered Entity that is: (i) the medical records and billing records about Individuals; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. As used herein the term "record" means any item, collection,

or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the Covered Entity.

1.7 "**Document Demand**" has the meaning set forth in Section 3.13.

1.8 "**Effective Date**" has the meaning set forth in the preamble.

1.9 "**Electronic PHI**" means information that comes within paragraphs 1(i) or 1(ii) of the definition of "PHI," as defined in 45 C.F.R. § 160.103, limited to the information created, received, maintained or transmitted by Business Associate on behalf of Covered Entity.

1.10 "**HIPAA**" has the meaning set forth in the Recitals.

1.11 "**HITECH Act**" means Title XIII and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law No. 111-5 and all regulations promulgated thereunder.

1.12 "**Individual**" means the person who is the subject of the PHI and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.13 "**PHI**" means Protected Health Information that is provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity.

1.14 "**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.

1.15 "**Protected Health Information**" (or "PHI") means any information, whether transmitted or maintained in electronic, written, oral, or any other form or medium, that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual; and (i) identifies the Individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

1.16 "**Required by Law**" has the same meaning as the term "'required by law" in 45 C.F.R. § 164.103.

1.17 "**Secretary**" means the Secretary of the U.S. Department of Health and Human Services or his or her designee.

1.18 "**Security Incident**" has the same meaning as the term "security incident" in 45 C.F.R. § 164.304.

1.19 "**Security Rule**" means the Security Standards and Implementation Specifications at 45 C.F.R. part 160 and part 164, subpart C.

1.20 "**Services Agreement**" has the meaning set forth in the Recitals.

1.21 "**Unsecured PHI**" or "**Unsecured PHI**" means PHI that is not secured through the use of a technology or methodology that the Secretary specifies in guidance renders PHI unusable, unreadable, or indecipherable to unauthorized Individuals, such as the guidance set forth in 74 Fed. Reg. 19006 (April 27, 2009) and updated in 74 Fed. Reg. 42740 (August 24, 2009).

1.22 Remaining Terms. Capitalized terms used, but not otherwise defined, in this Agreement have the meaning ascribed to them in HIPAA, the Privacy Rule, the Security Rule or the HITECH Act.

II. PERMITTED USES AND DISCLOSURES OF PHI

2.1 Services Agreement Uses and Disclosures. Business Associate may use or disclose PHI for purposes of performing its obligations and functions under the Services Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

2.2 Other Permitted Uses. If necessary, Business Associate may use PHI: (i) for the proper management and administration of the Business Associate; (ii) to carry out the legal responsibilities of the Business Associate; and (iii) for the provision of Data Aggregation services relating to the Health Care Operations of Covered Entity.

2.3 Other Permitted Disclosures. If necessary, Business Associate may disclose PHI for the purposes described in Section 2.2 above if: (i) the disclosure is Required by Law; or (ii) Business Associate obtains reasonable written assurance from the person or entity to whom it discloses the PHI that the PHI will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person or entity, and the person or entity notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

III. OBLIGATIONS OF BUSINESS ASSOCIATE

3.1 Compliance with Privacy Rule. Business Associate shall comply with all applicable provisions of the Privacy Rule in carrying out its obligations under the Services Agreement and this Agreement. Further, to the extent Business Associate is to carry out any of Covered Entity's obligations under subpart E of 45 CFR 164, Business Associate agrees to comply with the requirements of such subpart that apply to Covered Entity in the performance of such obligations.

3.2 Prohibition on Unauthorized Use or Disclosure. Business Associate shall not use or disclose PHI except as permitted by this Agreement or as Required by Law.

3.3 Minimum Necessary.

3.3.1 Business Associate shall limit its use and disclosure of PHI under this Agreement to the "minimum necessary," as set forth in guidance that the Secretary will issue regarding what constitutes "minimum necessary" under the Privacy Rule. Until the issuance of such guidance, Business Associate shall limit its use and disclosure of PHI, to the extent practicable, to the Limited Data Set (as that term is defined in 45 C.F.R.

§ 164.514(e)(2)), or, if needed, to the minimum necessary to accomplish the Business Associate's intended purpose. Business Associate may in good faith determine what constitutes the minimum necessary to accomplish the intended purpose of any disclosure of PHI.

3.3.2 Paragraph (a) above does not apply to: (1) disclosures to or requests by a health care provider for treatment; (2) uses or disclosures made to the Individual; (3) disclosures made pursuant to an authorization as set forth in 45 C.F.R. § 164.508; (4) disclosures made to the Secretary under 45 C.F.R. part 160, subpart C; (5) uses or disclosures that are Required by Law as described in 45 C.F.R. § 164.512(a); and (6) uses or disclosures that are required for compliance with applicable requirements of the Privacy Rule.

3.4 Safeguarding PHI; Security Regulations. Business Associate shall use appropriate administrative, physical, and technical safeguards and comply with the Security Rule with respect to Electronic PHI to prevent the use or disclosure of PHI other than as provided for by this Agreement.

3.5 Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Security Incident or a use or disclosure of PHI by Business Associate in violation of this Agreement.

3.6 Reporting. In the event that Business Associate becomes aware of a use or disclosure of PHI by Business Associate that is not permitted under this Agreement, Business Associate shall report such use or disclosure to the Covered Entity promptly in writing and in any event, within 5 days of becoming aware of the use or disclosure. Business Associate agrees to report to Covered Entity in writing any Security Incident of which it becomes aware, except that, for purposes of this reporting requirement the term "Security Incident" does not include inconsequential incidents that occur on a frequent basis such as scans or "pings" that are not allowed past Business Associate's firewall. Notwithstanding this Section 3.7, the Business Associate's reporting obligations regarding any ARRA Breach are set forth in Article IV.

3.7 Subcontractors. Business Associate shall ensure that all subcontractors or agents of Business Associate that create, receive, maintain or transmit PHI on behalf of the Business Associate agree in writing to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Business Associate shall ensure that all agents, including subcontractors, to whom it provides Electronic PHI, agree in writing to implement reasonable and appropriate safeguards to protect such Electronic PHI.

3.8 Access.

3.8.1 Within twenty (20) days of a request from Covered Entity, Business Associate shall furnish the PHI contained in a Designated Record Set that will enable the Covered Entity to respond to an Individual's request for inspection or copies of PHI about the Individual pursuant to 45 CFR § 164.524.

3.8.2 In the event an Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to the Covered Entity

immediately and take no direct immediate action on any such request. If the Covered Entity determines that an Individual is to be granted access to PHI, then Business Associate shall cooperate with the Covered Entity to provide to any Individual, at the Covered Entity's direction, any PHI requested by such Individual.

3.9 Amendment.

3.9.1 If the Covered Entity requests that Business Associate amend any Individual's PHI or a record regarding an Individual contained in a Designated Record Set, then Business Associate shall provide the relevant PHI to the Covered Entity for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526.

3.9.2 In the event an Individual requests directly to Business Associate that PHI be amended, Business Associate shall forward such request to the Covered Entity within ten (10) days of Business Associate's receipt of such request and shall take no direct immediate action on the request.

3.10 Records Availability. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining compliance with the Privacy Rule and the Security Rule.

3.11 Accounting of Disclosures.

3.11.1 If the Covered Entity requests that Business Associate furnish an accounting of disclosures of PHI made by Business Associate regarding an Individual during the six (6) years prior to the date on which the accounting was requested, then Business Associate shall, within fifteen (15) days of such request, make available to the Covered Entity such information as is in Business Associate's possession and is required for the Covered Entity to make the accounting required by 45 C.F.R. §164.528 and future regulations to be promulgated regarding accounting of disclosures.

3.11.2 In the event an Individual requests an accounting of disclosures directly from Business Associate, Business Associate shall within ten (10) days forward such request to the Covered Entity and shall take no direct action on the request.

3.12 Demands for Production of PHI.

3.12.1 Receipt by Business Associate. If Business Associate receives a subpoena, civil or administrative demand, or any other demand for production of PHI (a "Document Demand"), Business Associate shall provide a copy of such Document Demand to Covered Entity within five (5) days of receipt. To the extent the PHI that is the subject of the Document Demand is in the possession of Business Associate, and a response is warranted according to the standards contained in 45 C.F.R. § 164.512(e), Business Associate shall timely respond to the Document Demand.

3.12.2 Receipt by Covered Entity. If Covered Entity receives a Document Demand, Business Associate shall provide to Covered Entity any PHI responsive to such

Document Demand and assist and cooperate with Covered Entity in responding to such Document Demand in a timely manner and in accordance with the standards under 45 C.F.R. § 164.512(e).

3.13 Request for Restrictions on Disclosure of PHI. As required by Section 13405 of the HITECH Act and 45 CFR 164.522 (except as otherwise required by law), Business Associate shall comply with any request of an Individual for the Business Associate to restrict the disclosure of PHI of the Individual when the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment), and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

3.14 Remuneration for PHI.

3.14.1 Except as explicitly permitted in the Services Agreement and also set forth in paragraph (b) below, Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI of an Individual unless the Individual provided to the Covered Entity a valid authorization in accordance with 45 C.F.R. § 164.508 that specifically authorizes the Business Associate to exchange the PHI for remuneration.

3.14.2 Paragraph (a) above does not apply if the purpose of the exchange is: (1) for public health purposes pursuant to 45 CFR § 164.512(b) or § 164.514(e); (2) for research purposes pursuant to 45 CFR § 164.512(i) or § 164.514(e), where the only remuneration received by the Covered Entity or Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes; (3) for treatment and payment purposes pursuant to 45 CFR § 164.506(a); (4) for the sale, transfer, merger, or consolidation of all or part of the Covered Entity and for related due diligence as described in the HIPAA definition of health care operations and pursuant to 45 CFR § 164.506(a); (5) To or by a Business Associate for activities that the Business Associate undertakes on behalf of a Covered Entity (or on behalf of a Business Associate in the case of a subcontractor), pursuant to 45 CFR §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the Covered Entity to the Business Associate (or by the Business Associate to the subcontractor, if applicable), for the performance of such activities; (6) to an Individual, when the Individual requests access to his or her PHI pursuant to 45 CFR § 164.524 or when the Individual requests an accounting of disclosures pursuant to 45 CFR § 164.528; (7) for disclosures Required By Law; and (8) for any other purpose permitted by HIPAA where the only remuneration received by the Covered Entity or Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee expressly permitted by law.

3.15 Marketing Restrictions. Business associate shall ensure that any Marketing communications it makes on behalf of Covered Entity are in compliance with the rules governing marketing set forth in 45 C.F.R. 164.508(a)(3), including but not limited to the requirements that Business Associate must obtain an authorization from an Individual prior to making any marketing communication to such Individual.

3.16 Fundraising Limitations. Business Associate shall ensure that any fundraising communications Business Associate makes on behalf of the Covered Entity are in compliance with the rules governing fundraising communications set forth in 45 C.F.R. 164.514(f), including but not limited to the requirement that Business Associate must provide, with each fundraising communication made to an Individual, a clear and conspicuous opportunity for the recipient of the communication to elect not to receive any further fundraising communications. Business Associate shall ensure that all Individuals electing not to receive any further fundraising communications do not receive any further fundraising communications.

IV. ARRA BREACH NOTIFICATION.

4.1 Risk Assessment by Business Associate. If Business Associate becomes aware of a potential ARRA Breach, Business Associate shall complete a risk assessment of the potential ARRA Breach to determine whether the potential ARRA Breach is an ARRA Breach. Such risk assessment shall include at least all the factors identified in 45 CFR 164.402(2), as amended by the final rule published in the Federal Register on January 25, 2013 at 78 Fed. Reg. 5566.

4.2 Notification to Covered Entity. If, after completing such risk assessment, Business Associate concludes that there was an ARRA Breach, Business Associate shall notify the Covered Entity of the ARRA Breach as soon as reasonably possible, and in all cases within five (5) business days of the first day on which any employee, officer or agent of Business Associate either knows or by exercising reasonable diligence would have known that an ARRA Breach occurred. The notification to Covered Entity shall include, if known, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed during such ARRA Breach. The notification shall also include: (a) a brief description of what happened, including the date of the ARRA Breach and the date of the discovery of the ARRA Breach, if known; (b) a description of the types of Unsecured PHI that were involved in the ARRA Breach (such as whether the full name, social security number, date of birth, home address, account number, diagnosis disability code or other types of information were involved); (c) recommended steps that Individuals should take to protect themselves from potential harm resulting from the ARRA Breach; and (d) a brief description of what the Business Associate is doing to investigate the ARRA Breach, to mitigate harm to Individuals, and to protect against any further ARRA Breaches. Business Associate shall maintain evidence to demonstrate that any required risk assessment was completed and notification to the Covered Entity under this paragraph was made unless the Business Associate determines that a delayed notice (as described in Section 4.3) applies.

4.3 Delayed Notification to Covered Entity. Notwithstanding Section 4.2 above, if a law enforcement official states in writing to Business Associate that the notification to Covered Entity required under Section 4.2 would impede a criminal investigation or cause damage to national security, then Business Associate may delay the notification for any period of time set forth in the written statement of the law enforcement official. If the law enforcement official provides an oral statement, then Business Associate shall document the statement in writing, including the name of the law enforcement official making the statement, and may delay the notification required under Section 4.2 for no longer than thirty (30) days from the date of the oral statement, unless the law enforcement official provides a written statement during that time that specifies a different time period. Business Associate shall be obligated to maintain evidence to

demonstrate the reason for the delayed notification and that the required notification under this paragraph was made

4.4 Notification to Individuals, the Secretary and/or the Media. In the event of an ARRA Breach caused by Business Associate, its agents and/or subcontractors, Business Associate shall provide assistance to Covered Entity in making all ARRA Breach notifications. To the extent Covered Entity incurs expenses and costs to comply with its notification obligations with respect to an ARRA Breach by Business Associate, its agents and/or subcontractors, in addition to any other remedies that may be available to Covered Entity under this Agreement or any applicable law, Business Associate shall reimburse Covered Entity for all costs and expenses (including attorneys' fees) incurred by Covered Entity related to providing the notifications required under 45 C.F.R. §§ 164.404, 406 and 408. Notwithstanding the foregoing, if the parties agree that Business Associate will, on behalf of Covered Entity, and within the applicable time frames required by law under 45 C.F.R. §§ 164.404, 406 and 408, prepare and send out any and all required ARRA Breach notifications to Individuals, the Secretary and/or to the media, Business Associate shall prepare and send such ARRA Breach notifications at Business Associate's sole expense and in compliance with the requirements of 45 C.F.R. 164.404, 406 and 408, as applicable. However, any ARRA Breach notifications Business Associate would prepare and send on behalf of Covered Entity shall be subject to Covered Entity's review and pre-approval before the notifications are sent. Additionally, in the event of an ARRA Breach, Business Associate agrees to pay for the credit monitoring fees for affected Individuals for a period of at least two (2) years of credit monitoring.

V. TERM AND TERMINATION

5.1 Term. This Agreement is effective upon the effective date of the Services Agreement, and except for the rights and obligations set forth in this Agreement specifically surviving termination, shall terminate the later of the date the Services Agreement terminates or when all PHI is returned to Covered Entity or, with prior permission of Covered Entity, destroyed.

5.2 Termination for Cause. Notwithstanding any provision in this Agreement, Covered Entity may terminate this Agreement and the Services Agreement if Covered Entity determines, in its sole discretion, Business Associate has breached any provision of this Agreement or otherwise violated HIPAA, the Privacy Rule, the Security Rule or the HITECH Act. Covered Entity shall provide written notice to Business Associate with an opportunity for Business Associate to cure the breach or end the violation within ten (10) business days of such written notice, unless cure is not possible. If Business Associate fails to cure the breach or end the violation within the specified time period, or if cure is not possible, this Agreement and the Service Agreement shall automatically and immediately terminate, unless termination is infeasible.

5.3 Termination after Repeated Violations. Notwithstanding any provision in the Agreement, Covered Entity may terminate the Services Agreement and this Agreement if Covered Entity determines, in its sole discretion, that Business Associate has repeatedly breached any provision of this Agreement or otherwise violated HIPAA, the Privacy Rule, the Security Rule or the HITECH Act, irrespective of whether, or how promptly, Business Associate may remedy such violation after being notified of the same.

5.4 Obligations Upon Termination. Business Associate's obligations to protect the privacy and security of PHI shall be continuous and shall survive termination, cancellation, expiration or other conclusion of this Agreement or the Services Agreement. Upon termination of this Agreement, Business Associate will forward to Covered Entity, or to Covered Entity's designee, the records necessary for continued administration of Covered Entity as directed by Covered Entity. After the forwarding of said records, whatever PHI remains with Business Associate will be subject to the following:

5.4.1 Except as provided in paragraph (b) of this Section 5.4, upon termination, cancellation, expiration or other conclusion of this Agreement, for any reason, Business Associate shall return or, if Covered Entity gives written permission, destroy, PHI in whatever form or medium and retain no copies of such PHI. Business Associate will complete such return or destruction as soon as possible, but in no event later than sixty (60) days from the date of the termination of this Agreement. Within ten (10) days of the return or destruction of all PHI by Business Associate, Business Associate shall provide written certification to Covered Entity that the return or destruction of PHI has been completed.

5.4.2 In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VI. INDEMNIFICATION; INSURANCE

6.1 Indemnification by Business Associate. Business Associate will indemnify and hold harmless Covered Entity, and any affiliate, officer, director, employee or agent of Covered Entity from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any use or disclosure of PHI that violates or is not permitted by this Agreement, HIPAA, the Privacy Rule, the Security Rule or the HITECH Act, or other breach of this Agreement by Business Associate or any subcontractor or agent of Business Associate.

6.2 Right to Tender or Undertake Defense. If Covered Entity is named as a party in any judicial, administrative or other proceeding arising out of or in connection with any non-permitted or violating use or disclosure of PHI or other breach of this Agreement by Business Associate or any subcontractor or agent of Business Associate, Covered Entity shall have the option at any time either to: (i) tender its defense to Business Associate, in which case Business Associate will provide qualified attorneys, consultants, and other appropriate professionals to represent Covered Entity's interests at Business Associate's expense; or (ii) undertake its own defense, choosing the attorneys, consultants, and other appropriate professionals to represent its interests, in which case Business Associate will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants, and other professionals.

6.3 Right to Control Resolution. Covered Entity has the sole right and discretion to settle, compromise or otherwise resolve any and all claims, causes of actions, liabilities or damages against it, notwithstanding that Covered Entity may have tendered its defense to Business Associate. Any such resolution will not relieve Business Associate of its obligation to indemnify Covered Entity under this Agreement.

6.4 Insurance. Upon request, Business Associate shall obtain and maintain insurance coverage against improper uses and disclosures of PHI by Business Associate, naming Covered Entity as an additional named insured. Upon request, Business Associate shall provide a certificate evidencing such insurance coverage.

6.5 Conflicts. With respect to any breaches or violations of this Agreement, the provisions in this Section 6 supersede any inconsistent terms contained in the Services Agreement.

VII. GENERAL PROVISIONS

7.1 Effect. The terms and provisions of this Agreement supersede any other conflicting or inconsistent terms and provisions in any agreements between the parties, including all exhibits or other attachments thereto and all documents incorporated therein by reference.

7.2 Amendment. Business Associate and the Covered Entity agree to amend this Agreement to the extent necessary to allow either party to comply with HIPAA, the Privacy Rule, the Security Rule, or the HITECH Act. All such amendments shall be made in a writing signed by both parties.

7.3 No Third Party Beneficiaries. This Agreement is intended for the benefit of Business Associate and Covered Entity only. Nothing express or implied is intended to confer or create, nor be interpreted to confer or create, any rights, remedies, obligations or liabilities to or for any third party beneficiary, including without limitation Individuals who are the subject of PHI.

7.4 Severability. In the event that any provision of this Agreement violates any applicable statute, ordinance, or rule of law in any jurisdiction that governs this Agreement, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this Agreement.

7.5 No Waiver. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.

7.6 Assignment. This Agreement may not be assigned by either party without the prior written consent of the other party; provided, however, that the parties shall cooperate to assign this Agreement as appropriate if the Services Agreement is assigned.

7.7 Relationship of the Parties. Business Associate and Covered Entity are independent contractors and all acts performed by Business Associate are performed solely in its capacity as an independent contractor.

7.8 Counterparts; Facsimile Signature. This Agreement may be executed by facsimile and/or in counterparts, each of which shall be an original and all of which together shall constitute one and the same binding instrument.

7.9 Notification

7.9.1 Business Associate. To the extent notice is required to be provided by Covered Entity to Business Associate under any provision in this Agreement, notice shall be provided to:

Russell Wood
russell.wood@cicsmhds.org
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010
Phone 515-663-2928

7.9.2 Covered Entity. To the extent notice is required to be provided by Business Associate to Covered Entity under any provision in this Agreement, notice shall be provided to:

Alissa Wignall
Alissa.wignall@storycountyiowa.gov
900 6th St.
Nevada, IA 50201
Phone 515-382-7204
Fax 515-382-7206

7.10 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA, the Privacy Rule, the Security Rule, and the HITECH Act.

INTENDING TO BE LEGALLY BOUND, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

BUSINESS ASSOCIATE

Central Iowa Community Services

By: _____

Print Name: _____

Title: _____

Date: _____

COVERED ENTITY

Story County, Iowa

By: _____

Print Name: LINDA MURKEN

Title: VICE-CHAIR

Date: 6-14-22

May 2022 Expenditure Report

FY 2022	CICS MHDS Region	Monthly Expenditures	YTD Expenditures	FY22 Budget	Budget Remaining	% of Budget Used
Core Domains						
COA	**Treatment**					
42305	Mental health outpatient therapy	$ 2,777	$ 24,113	$ 150,000	$ 125,887	16%
42306	Medication prescribing & management	$ 13,890	$ 27,780	$ 20,000	$ (7,780)	139%
43301	Assessment & evaluation	$ -	$ -	$ 20,000	$ 20,000	0%
71319	Mental health inpatient therapy-MHI	$ -	$ 80,142	$ 200,000	$ 119,858	40%
73319	Mental health inpatient therapy	$ 135	$ 135	$ 25,000	$ 24,865	1%
	Crisis Services					
32322	Personal emergency response system	$ -	$ -	$ 5,000	$ 5,000	0%
44301	Crisis evaluation	$ 73,761	$ 576,825	$ 625,000	$ 48,175	92%
44302	23 hour crisis observation & holding	$ -	$ -	$ 40,000	$ 40,000	0%
44305	24 hour access to crisis response	$ 89	$ 89	$ -	$ (89)	
44307	Mobile response	$ 94,803	$ 1,021,848	$ 950,000	$ (71,848)	108%
44312	Crisis Stabilization community-based services	$ 17,953	$ 205,163	$ 250,000	$ 44,837	82%
44313	Crisis Stabilization residential services	$ 664,552	$ 818,862	$ 150,000	$ (668,862)	546%
44396	Access Centers: start-up / sustainability	$ -	$ -	$ 500,000	$ 500,000	0%
	Support for Community Living					
32320	Home health aide	$ -	$ -	$ -	$ -	
32325	Respite	$ 1,278	$ 4,590	$ 5,000	$ 410	92%
32328	Home & vehicle modifications		$ -	$ -	$ -	
32329	Supported community living	$ 74,825	$ 574,306	$ 1,100,000	$ 525,694	52%
42329	Intensive residential services	$ -	$ -	$ 500,000	$ 500,000	0%
	Support for Employment					
50362	Prevocational services	$ 857	$ 8,133	$ 25,000	$ 16,867	33%
50364	Job development		$ -	$ -	$ -	
50367	Day habilitation	$ 10,509	$ 103,264	$ 225,000	$ 121,736	46%
50368	Supported employment	$ 14,065	$ 114,668	$ 100,000	$ (14,668)	115%
50369	Group Supported employment-enclave	$ 1,207	$ 13,391	$ 20,000	$ 6,609	67%
	Recovery Services					
45323	Family support	$ 4,373	$ 41,433	$ 25,000	$ (16,433)	166%
45366	Peer support	$ -	$ 3,719	$ 20,000	$ 16,281	19%
	Service Coordination					
21375	Case management		$ -	$ -	$ -	
24376	Health homes	$ -	$ -	$ -	$ -	
	Sub-Acute Services					
63309	Subacute services-1-5 beds		$ -	$ 100,000	$ 100,000	0%
64309	Subacute services-6 and over beds	$ 61,450	$ 274,699	$ 100,000	$ (174,699)	275%
	Core Evidenced Based Treatment					
04422	Education & Training Services - provider competency	$ -	$ -	$ 15,000	$ 15,000	0%
32396	Supported housing		$ -	$ -	$ -	
42398	Assertive community treatment (ACT)	$ 17,110	$ 117,171	$ 125,000	$ 7,829	94%
45373	Family psychoeducation	$ -	$ -	$ 10,000	$ 10,000	0%
	Core Domains Total	**$ 1,053,633**	**$ 4,010,331**	**$ 5,305,000**	**$ 1,294,669**	**76%**
Mandated Services						
46319	Oakdale	$ -	$ -	$ 50,000	$ 50,000	0%
72319	State resource centers		$ -	$ -	$ -	
74XXX	Commitment related (except 301)	$ 33,554	$ 242,377	$ 400,000	$ 157,623	61%
75XXX	Mental health advocate	$ 21,526	$ 216,719	$ 250,000	$ 33,281	87%
	Mandated Services Total	**$ 55,079**	**$ 459,096**	**$ 700,000**	**$ 240,904**	**66%**
Additional Core Domains						
	Justice system-involved services					
25xxx	Coordination services	$ 25,961	$ 280,776	$ 600,000	$ 319,224	47%
44346	24 hour crisis line**	$ -	$ -	$ -	$ -	
44366	Warm line**	$ -	$ -	$ 10,000	$ 10,000	0%
46305	Mental health services in jails	$ 14,604	$ 120,149	$ 250,000	$ 129,851	48%
46399	Justice system-involved services-other	$ -	$ -	$ -	$ -	
46422	Crisis prevention training	$ 21,504	$ 21,504	$ 25,000	$ 3,496	86%
46425	Mental health court related costs	$ -	$ -	$ -	$ -	
74301	Civil commitment prescreening evaluation	$ -	$ -	$ 5,000	$ 5,000	0%
	Additional Core Evidenced based treatment					
42366	Peer self-help drop-in centers	$ 62,689	$ 723,612	$ 785,000	$ 61,388	92%
42397	Psychiatric rehabilitation (IPR)	$ 1,868	$ 13,944	$ 60,000	$ 46,056	23%
	Additional Core Domains Total	**$ 126,627**	**$ 1,159,985**	**$ 1,735,000**	**$ 575,015**	**67%**
Other Informational Services						
03371	Information & referral	$ 160	$ 909	$ -	$ (909)	
04372	Planning and/or Consultation (client related)		$ -	$ -	$ -	
04377	Provider Incentive Payment		$ -	$ -	$ -	
04399	Consultation Other		$ -	$ -	$ -	
04429	Planning and Management Consultants (non-client related)	$ -	$ -	$ 50,000	$ 50,000	0%
05373	Public education	$ 5,930	$ 118,449	$ 200,000	$ 81,551	59%
	Other Informational Services Total	**$ 6,090**	**$ 119,358**	**$ 250,000**	**$ 130,642**	**48%**
Essential Community Living Support Services						

May 2022 Expenditure Report

FY 2022	CICS MHDS Region	Monthly Expenditures	YTD Expenditures	FY22 Budget	Budget Remaining	% of Budget Used
06399	Academic services		$ -	$ -	$ -	
22XXX	Services management	$ 128,102	$ 1,499,938	$ 1,950,000	$ 450,062	77%
23376	Crisis care coordination	$ -	$ -	$ -	$ -	
23399	Crisis care coordination other		$ -	$ -	$ -	
24399	Health home other		$ -	$ -	$ -	
31XXX	Transportation	$ 25,263	$ 187,077	$ 250,000	$ 62,923	75%
32321	Chore services		$ -	$ -	$ -	
32326	Guardian/conservator	$ -	$ 300	$ 5,000	$ 4,700	6%
32327	Representative payee	$ 816	$ 9,051	$ 20,000	$ 10,949	45%
32335	CDAC		$ -	$ -	$ -	#DIV/0!
32399	Other support		$ -	$ -	$ -	#DIV/0!
33330	Mobile meals		$ -	$ -	$ -	
33340	Rent payments (time limited)	$ 1,387	$ 31,602	$ 200,000	$ 168,398	
33345	Ongoing rent subsidy	$ -	$ 770	$ -	$ (770)	
33399	Other basic needs	$ 1,643	$ 28,251	$ 80,000	$ 51,749	
41305	Physiological outpatient treatment	$ 50	$ 50	$ 5,000	$ 4,950	1%
41306	Prescription meds	$ 551	$ 2,404	$ 15,000	$ 12,596	16%
41307	In-home nursing		$ -	$ -	$ -	
41308	Health supplies		$ -	$ -	$ -	
41399	Other physiological treatment		$ -	$ -	$ -	
42309	Partial hospitalization		$ -	$ -	$ -	
42310	Transitional living program	$ -	$ 58,609	$ 400,000	$ 341,391	15%
42363	Day treatment		$ -	$ -	$ -	
42396	Community support programs	$ -	$ 531	$ 10,000	$ 9,469	5%
42399	Other psychotherapeutic treatment	$ -	$ -	$ -	$ -	
43399	Other non-crisis evaluation		$ -	$ -	$ -	
44304	Emergency care		$ -	$ -	$ -	
44399	Other crisis services		$ -	$ -	$ -	
45399	Other family & peer support		$ -	$ -	$ -	
46306	Psychiatric medications in jail	$ 4,103	$ 36,330	$ 50,000	$ 13,670	73%
50361	Vocational skills training		$ -	$ -	$ -	
50365	Supported education		$ -	$ -	$ -	
50399	Other vocational & day services		$ -	$ -	$ -	
63XXX	RCF 1-5 beds *(63314, 63315 & 63316)*	$ -	$ -	$ -	$ -	
63XXX	ICF 1-5 beds *(63317 & 63318)*		$ -	$ -	$ -	
63329	SCL 1-5 beds		$ -	$ -	$ -	
63399	Other 1-5 beds		$ -	$ -	$ -	
	Essential Comm Living Support Services Total	**$ 161,916**	**$ 1,854,913**	**$ 2,985,000**	**$ 1,130,087**	**62%**
Other Congregate Services						
50360	Work services (work activity/sheltered work)	$ -	$ -	$ -	$ -	
64XXX	RCF 6 and over beds *(64314, 64315 & 64316)*	$ 88,248	$ 591,440	$ 900,000	$ 308,560	66%
64XXX	ICF 6 and over beds *(64317 & 64318)*		$ 3,896	$ -	$ (3,896)	
64329	SCL 6 and over beds	$ 17,038	$ 124,133	$ -	$ (124,133)	
64399	Other 6 and over beds	$ -	$ -	$ -	$ -	
	Other Congregate Services Total	**$ 105,287**	**$ 719,469**	**$ 900,000**	**$ 180,531**	**80%**
Administration						
11XXX	Direct Administration	$ 89,407	$ 1,251,929	$ 1,500,000	$ 248,071	83%
12XXX	Purchased Administration	$ 6,784	$ 39,148	$ 125,000	$ 85,852	31%
	Administration Total	**$ 96,191**	**$ 1,291,077**	**$ 1,625,000**	**$ 333,923**	**79%**
	Regional Totals	**$ 1,604,823.40**	**$ 9,614,230.24**	**$ 13,500,000**	**$ 3,885,770**	**71%**
						92%
(45XX-XXX)	**County Provided Case Management**					
(46XX-XXX)	**County Provided Services**					

Transfer Numbers (Expenditures should only be counted when final expenditure is made for services/administration. Transfers are eliminated from budget to show true regional finances)

13951	**Distribution to MHDS regional fiscal agent from member county**	$ -	$ -			
14951	**MHDS fiscal agent reimbursement to MHDS regional member county**	$ -	$ -			
15481	**Distribution to Other MHDS Region (CARES)**	$ -	$ -			

** 24 hour crisis line and warm line are transitioning from additional core to state wide core services with state funding.

Disbursement Date 05/31/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
7147 V	60	Linn Adams		Services Management - Mil	41500	04022	413	62			90.70
7147 V	60	Linn Adams		Services Management - Mil	41500	04222	413	62			90.69
7147 V	60	Linn Adams		Services Management - Mil	41500	04322	413	62			80.69
				Disbursement# 5322		Disbursement Total					262.08
7148 V	169	Amazon Capital Services		Direct Admin - Stationary	41500	04411	260	62			6.25
7148 V	169	Amazon Capital Services		Direct Admin - Stationary	41500	04411	260	62			21.99
7148 V	169	Amazon Capital Services		Direct Admin - Informatio	41500	04411	262	62			72.45
				Disbursement# 5323		Disbursement Total					100.69
7152 V	520	Auditor Of State		Purchased Admin - Account	41500	04412	420	62			6784.00
				Disbursement# 5324		Disbursement Total					6,784.00
7156 V	884	Boone County Jail		Prescription Medication (	41500	04046	306	62			4.89
				Disbursement# 5325		Disbursement Total					4.89
7194 V	72147	CDW Government Inc.		Direct Admin - Informatio	41500	04411	632	62			1562.28
				Disbursement# 5326		Disbursement Total					1,562.28
7157 V	1327	Center Associates		Psychotherapeutic Treatme	41500	04042	306	62			72.45
7157 V	1327	Center Associates		Psychotherapeutic Treatme	41500	04042	306	62			72.45
7157 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			144.90
7157 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			376.99
7157 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			72.45
7157 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			304.54
				Disbursement# 5327		Disbursement Total					1,043.78
7158 V	1362	Central Iowa Psychological		Mental Health Services in	41500	04046	305	62			114.17
7158 V	1362	Central Iowa Psychological		Mental Health Services in	41500	04046	305	62			155.61
				Disbursement# 5328		Disbursement Total					269.78
7159 V	1372	Central Services 2-5-12		Direct Admin - Building (	41500	04411	450	62			750.00
				Disbursement# 5329		Disbursement Total					750.00
7160 V	1473	ChildServe Inc.		Support Services - Respit	41500	04232	325	62			204.80
				Disbursement# 5330		Disbursement Total					204.80
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			40.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			40.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			40.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			60.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			80.00

Disbursement Date 05/31/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7149 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7150 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			80.00
7150 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			40.00
7150 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			60.00
7150 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
				Disbursement#	5331	Disbursement Total					660.00
7154 V	745	Counsel Off. & Document		Direct Admin - Office Equ	41500	04411	444	62			23.02
				Disbursement#	5332	Disbursement Total					23.02
7161 V	1762	Crossroads Mental Hlth Ctr		Crisis Evaluation	41500	04044	301	62			300.00
7161 V	1762	Crossroads Mental Hlth Ctr		Mental Health Services in	41500	04046	305	62			155.61
7161 V	1762	Crossroads Mental Hlth Ctr		Mental Health Services in	41500	04046	305	62			155.61
7161 V	1762	Crossroads Mental Hlth Ctr		Mental Health Services in	41500	04046	305	62			155.61
				Disbursement#	5333	Disbursement Total					766.83
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2030.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2320.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			870.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2030.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2320.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			870.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1450.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2900.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2320.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2900.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2320.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			3190.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			3190.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2900.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2030.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			870.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			580.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2900.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2320.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04244	301	62			290.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04244	301	62			290.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			900.00

Disbursement Date 05/31/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line	Amount
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				290.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
				Disbursement#	5334	Disbursement Total						62,700.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				320.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				640.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				320.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04744	301	62				290.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				320.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
				Disbursement#	5335	Disbursement Total						6,850.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				290.00
7162 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				580.00
7163 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				160.00
7163 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				290.00
7163 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				290.00
7163 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62				290.00

Disbursement Date 05/31/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
				Disbursement# 5336		Disbursement Total					2,060.00
7182 V	5696	Eyerly Ball CMHS		Crisis Stabilization Comm	41500	04044	312	62			8902.35
7182 V	5696	Eyerly Ball CMHS		Crisis Stabilization Comm	41500	04044	312	62			8902.36
7182 V	5696	Eyerly Ball CMHS		Mobile Response	41500	04044	307	62			85560.65
7182 V	5696	Eyerly Ball CMHS		Assertive Community Treat	41500	04042	398	62			4640.00
				Disbursement# 5337		Disbursement Total					108,005.36
7193 V	72119	Franklin County Sheriff's Off.		Commitment - Sheriff Tran	41500	04074	353	62			161.96
7193 V	72119	Franklin County Sheriff's Off.		Commitment - Sheriff Tran	41500	04074	353	62			98.45
				Disbursement# 5338		Disbursement Total					260.41
7164 V	2436	Friendship Ark Inc.		Support Services - Suppor	41500	04032	329	62			691.92
7164 V	2436	Friendship Ark Inc.		Support Services - Suppor	41500	04332	329	62			5267.40
				Disbursement# 5339		Disbursement Total					5,959.32
7166 V	2924	Frontier Communications		Direct Admin - Telecommun	41500	04411	414	62			146.39
				Disbursement# 5340		Disbursement Total					146.39
7172 V	3744	Greene Co. Medical Center		Psychotherapeutic Treatme	41500	04042	306	62			11250.00
				Disbursement# 5341		Disbursement Total					11,250.00
7178 V	4984	Lisa Hill		Direct Admin - Mileage &	41500	04411	413	62			23.40
				Disbursement# 5342		Disbursement Total					23.40
7167 V	3019	Hillcrest Family Services		Comm Based Settings (6+ B	41500	04064	314	62			2423.40
7167 V	3019	Hillcrest Family Services		Comm Based Settings (6+ B	41500	04064	314	62			865.50
7167 V	3019	Hillcrest Family Services		Comm Based Settings (6+ B	41500	04064	314	62			7929.90
7167 V	3019	Hillcrest Family Services		Comm Based Settings (6+ B	41500	04064	314	62			1817.55
7167 V	3019	Hillcrest Family Services		Comm Based Settings (6+ B	41500	04064	314	62			2803.13
				Disbursement# 5343		Disbursement Total					15,839.48
7179 V	5137	HIRTA Public Transit		Transportation - General	41500	04031	354	62			484.38
7179 V	5137	HIRTA Public Transit		Transportation - General	41500	04031	354	62			346.17
7179 V	5137	HIRTA Public Transit		Transportation - General	41500	04031	354	62			209.64
				Disbursement# 5344		Disbursement Total					1,040.19
7168 V	3129	Liza Howard		Services Management - Mil	41500	04022	413	62			194.74
7168 V	3129	Liza Howard		Services Management - Mil	41500	04222	413	62			189.02
7168 V	3129	Liza Howard		Services Management - Mil	41500	04322	413	62			189.01
				Disbursement# 5345		Disbursement Total					572.77
7196 V	83184	Hy-Vee Accts Rcvble		Physiological Treatment -	41500	04041	306	62			349.53
				Disbursement# 5346		Disbursement Total					349.53
7169 V	3203	Hy-Vee Pharmacy-Indianola		Physiological Treatment -	41500	04041	306	62			129.85
7169 V	3203	Hy-Vee Pharmacy-Indianola		Physiological Treatment -	41500	04041	306	62			72.05
				Disbursement# 5347		Disbursement Total					201.90
7170 V	3227	Imagine The Possibilities Inc		Support Services - Suppor	41500	04232	329	62			1376.16

Disbursement Date 05/31/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
7170 V	3227	Imagine The Possibilities Inc		Day Habilitation	41500	04250	367	62			795.68
7170 V	3227	Imagine The Possibilities Inc		Support Services - Suppor	41500	04332	329	62			1659.20
7170 V	3227	Imagine The Possibilities Inc		Day Habilitation	41500	04350	367	62			884.16
7170 V	3227	Imagine The Possibilities Inc		Voc/Day - Individual Supp	41500	04350	368	62			905.60
7170 V	3227	Imagine The Possibilities Inc		Day Habilitation	41500	04750	367	62			355.75
				Disbursement# 5348		Disbursement Total					5,976.55
7155 V	764	Infinity Health		Physiological Treatment -	41500	04041	305	62			50.00
7155 V	764	Infinity Health		Mobile Response	41500	04044	307	62			55.00
7155 V	764	Infinity Health		Crisis Stabilization Comm	41500	04044	312	62			148.20
				Disbursement# 5349		Disbursement Total					253.20
7171 V	3620	Jasper County Sheriff		Crisis Prevention Trainin	41500	04046	422	62			1282.21
				Disbursement# 5350		Disbursement Total					1,282.21
7175 V	4400	Mainstream Living		Day Habilitation	41500	04350	367	62			515.76
7175 V	4400	Mainstream Living		Voc/Day - Group Supported	41500	04350	369	62			128.10
				Disbursement# 5351		Disbursement Total					643.86
7176 V	4443	Marshall County		Prescription Medication (	41500	04046	306	62			847.30
7176 V	4443	Marshall County		Commitment - Sheriff Tran	41500	04074	353	62			31.00
7176 V	4443	Marshall County		Commitment - Sheriff Tran	41500	04074	353	62			61.00
				Disbursement# 5352		Disbursement Total					939.30
7177 V	4901	Medicap Pharmacy 8095		Prescription Medication (	41500	04046	306	62			439.21
				Disbursement# 5353		Disbursement Total					439.21
7180 V	5370	ODP Business Solutions, LLC		Direct Admin - Stationary	41500	04411	260	62			10.87
				Disbursement# 5354		Disbursement Total					10.87
7181 V	5448	One Vision-Opportunity Village		Voc/Day - Individual Supp	41500	04250	368	62			747.79
7181 V	5448	One Vision-Opportunity Village		Support Services - Suppor	41500	04332	329	62			413.23
				Disbursement# 5355		Disbursement Total					1,161.02
7165 V	2872	Optimae LifeServices, Inc.		Justice System Involved C	41500	04025	376	62			5882.00
				Disbursement# 5356		Disbursement Total					5,882.00
7174 V	4316	Orchard Place CCR&R		Psychotherapeutic Treatme	41500	04042	305	62			72.47
7174 V	4316	Orchard Place CCR&R		Psychotherapeutic Treatme	41500	04042	305	62			72.47
7174 V	4316	Orchard Place CCR&R		Psychotherapeutic Treatme	41500	04042	305	62			72.47
7174 V	4316	Orchard Place CCR&R		Psychotherapeutic Treatme	41500	04042	305	62			72.47
				Disbursement# 5357		Disbursement Total					289.88
7195 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	366	62			3898.36
7195 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04242	366	62			1158.96
7195 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04342	366	62			368.76
7195 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04742	366	62			597.04
				Disbursement# 5358		Disbursement Total					6,023.12
7183 V	5748	Productive Corporation		Direct Admin - Informatio	41500	04411	632	62			2079.00

Disbursement Date 05/31/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
				Disbursement# 5359		Disbursement Total					2,079.00
7184 V	6420	REM Ia Developmental Srv, Inc		Day Habilitation	41500	04750	367	62			542.08
				Disbursement# 5360		Disbursement Total					542.08
7185 V	6465	Scenic Acres		Comm Based Settings (6+ B	41500	04064	329	62			236.88
7185 V	6465	Scenic Acres		Comm Based Settings (6+ B	41500	04064	329	62			262.26
7185 V	6465	Scenic Acres		Comm Based Settings (6+ B	41500	04064	329	62			4058.40
				Disbursement# 5361		Disbursement Total					4,557.54
7186 V	7125	Story County Treasurer		Prescription Medication (	41500	04046	306	62			4.79-
7186 V	7125	Story County Treasurer		Prescription Medication (	41500	04046	306	62			111.04
				Disbursement# 5362		Disbursement Total					106.25
7151 V	367	Betsy Stursma		Direct Admin - Mileage &	41500	04411	413	62			424.13
				Disbursement# 5363		Disbursement Total					424.13
7187 V	7202	Thrifty White Pharmacy		Prescription Medication (	41500	04046	306	62			229.33
7188 V	7202	Thrifty White Pharmacy		Prescription Medication (	41500	04046	306	62			30.20
				Disbursement# 5364		Disbursement Total					259.53
7189 V	7409	Treasurer, State of Iowa		Commitment - Other	41500	04074	399	62			3333.33
7189 V	7409	Treasurer, State of Iowa		Commitment - Other	41500	04074	399	62			3333.33
7189 V	7409	Treasurer, State of Iowa		Commitment - Other	41500	04074	399	62			3333.33
				Disbursement# 5365		Disbursement Total					9,999.99
7173 V	4112	Patti Treibel-Leeds		Direct Admin - Mileage &	41500	04411	413	62			573.89
				Disbursement# 5366		Disbursement Total					573.89
7190 V	7498	U.S. Cellular		Direct Admin - Telecommun	41500	04411	414	62			721.06
				Disbursement# 5367		Disbursement Total					721.06
7153 V	700	UnityPoint Health		Assertive Community Treat	41500	04042	398	62			6960.00
				Disbursement# 5368		Disbursement Total					6,960.00
7191 V	7680	Warren County Sheriff		Commitment - Sheriff Tran	41500	04074	353	62			61.00
7191 V	7680	Warren County Sheriff		Commitment - Sheriff Tran	41500	04074	353	62			32.00
				Disbursement# 5369		Disbursement Total					93.00
7192 V	7696	Webster County Sheriff		Commitment - Sheriff Tran	41500	04074	353	62			3.00
7192 V	7696	Webster County Sheriff		Commitment - Sheriff Tran	41500	04074	353	62			9.00
7192 V	7696	Webster County Sheriff		Commitment - Sheriff Tran	41500	04074	353	62			3.00
				Disbursement# 5370		Disbursement Total					15.00

49	Total Disbursements	276,923.59
0	Total ACH	.00
0	Total EFT	.00
49	Grand Total	276,923.59
	Credits/Refunds Included	4.79

Disbursement Date 05/31/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line	Amount

Totals by Fund

41500	Central Iowa Community Service	276,923.59
	Final Total	276,923.59

End of report

Disbursement Date 06/14/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
7400 V	15	Abbe Center for Community		Comm Based Settings (6+ B	41500	04064	314	62			1039.43
				Disbursement# 5372		Disbursement Total					1,039.43
7401 V	169	Amazon Capital Services		Direct Admin - Stationary	41500	04411	260	62			46.82
7401 V	169	Amazon Capital Services		Direct Admin - Stationary	41500	04411	260	62			427.32
7401 V	169	Amazon Capital Services		Direct Admin - Stationary	41500	04411	260	62			14.89
7401 V	169	Amazon Capital Services		Direct Admin - Stationary	41500	04411	260	62			49.49
7401 V	169	Amazon Capital Services		Direct Admin - Stationary	41500	04411	260	62			43.62
				Disbursement# 5373		Disbursement Total					582.14
7416 V	1849	Branstad & Olson Law		Commitment - Legal Repres	41500	04074	393	62			132.00
				Disbursement# 5374		Disbursement Total					132.00
7409 V	1230	Capstone Behavioral Healthcare		Crisis Evaluation	41500	04044	301	62			692.52
7409 V	1230	Capstone Behavioral Healthcare		Crisis Evaluation	41500	04044	301	62			346.26
7409 V	1230	Capstone Behavioral Healthcare		Support Services - Suppor	41500	04032	329	62			962.23
7409 V	1230	Capstone Behavioral Healthcare		Mental Health Services in	41500	04046	305	62			59.43
7409 V	1230	Capstone Behavioral Healthcare		Mental Health Services in	41500	04046	305	62			59.43
7409 V	1230	Capstone Behavioral Healthcare		Psychotherapeutic Treatme	41500	04042	306	62			625.00
7409 V	1230	Capstone Behavioral Healthcare		Psychotherapeutic Treatme	41500	04042	305	62			833.34
7409 V	1230	Capstone Behavioral Healthcare		Justice System Involved C	41500	04025	376	62			6293.00
7409 V	1230	Capstone Behavioral Healthcare		Psychotherapeutic Treatme	41500	04042	366	62			5123.70
7409 V	1230	Capstone Behavioral Healthcare		Psychotherapeutic Treatme	41500	04242	366	62			1463.92
7409 V	1230	Capstone Behavioral Healthcare		Psychotherapeutic Treatme	41500	04342	366	62			329.38
7409 V	1230	Capstone Behavioral Healthcare		Psychotherapeutic Treatme	41500	04042	366	62			7160.68
7409 V	1230	Capstone Behavioral Healthcare		Psychotherapeutic Treatme	41500	04242	366	62			227.32
				Disbursement# 5375		Disbursement Total					24,176.21
7402 V	198	Carr Law Firm PLC		Commitment - Legal Repres	41500	04074	393	62			269.01
7402 V	198	Carr Law Firm PLC		Commitment - Legal Repres	41500	04074	393	62			181.35
7402 V	198	Carr Law Firm PLC		Commitment - Legal Repres	41500	04074	393	62			78.34
7402 V	198	Carr Law Firm PLC		Commitment - Legal Repres	41500	04074	393	62			98.69
				Disbursement# 5376		Disbursement Total					627.39
7450 V	72147	CDW Government Inc.		Direct Admin - Informatio	41500	04411	632	62			1563.50
				Disbursement# 5377		Disbursement Total					1,563.50
7418 V	2097	Cedar Valley Ranch, Inc.		Comm Based Settings (6+ B	41500	04064	314	62			4867.62
				Disbursement# 5378		Disbursement Total					4,867.62
7411 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			232.09
7411 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			72.45
7411 V	1327	Center Associates		Psychotherapeutic Treatme	41500	04042	306	62			14.40
7411 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			72.45
7411 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			304.54
7411 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			72.45
7411 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			304.54
7411 V	1327	Center Associates		Mental Health Services in	41500	04046	305	62			72.45
				Disbursement# 5379		Disbursement Total					1,145.37

Disbursement Date 06/14/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line	Amount
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				390.08
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				247.05
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				234.05
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				364.07
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				416.08
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				390.08
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				234.05
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				286.06
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				468.09
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				338.07
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				299.06
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				182.04
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				312.06
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				442.09
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				364.07
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				390.08
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				455.09
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				208.04
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				390.08
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				455.09
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				416.08
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				637.12
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				468.09
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				234.05
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				208.04
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				494.10
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				260.05
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				234.05
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				442.09
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				728.15
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				858.17
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				312.06
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				260.05
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				559.11
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				403.08
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				299.06
				Disbursement# 5380		Disbursement Total						13,678.73
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				247.05
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				182.04
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				442.09
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				429.08
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				481.09
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62				338.07
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				273.05
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				403.08
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				208.04
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				351.07
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				312.06
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62				182.04

Disbursement Date 06/14/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			962.20
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			143.03
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			676.14
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			364.07
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			494.10
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			338.07
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62			234.05
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62			182.04
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62			234.05
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			507.10
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			364.07
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			338.07
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			208.04
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			338.07
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			286.06
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			247.05
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			325.06
7412 V	1349	Central Iowa Detention		Transportation - General	41500	04031	354	62			208.04
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62			351.07
7412 V	1349	Central Iowa Detention		Commitment - Sheriff Tran	41500	04074	353	62			416.08
				Disbursement# 5381		Disbursement Total					11,065.22
7414 V	1362	Central Iowa Psychological		Mental Health Services in	41500	04046	305	62			208.29
7414 V	1362	Central Iowa Psychological		Mental Health Services in	41500	04046	305	62			155.61
				Disbursement# 5382		Disbursement Total					363.90
7413 V	1361	Central Iowa Recovery Inc.		Psychotherapeutic Treatme	41500	04042	366	62			2469.93
7413 V	1361	Central Iowa Recovery Inc.		Psychotherapeutic Treatme	41500	04242	366	62			4940.07
7413 V	1361	Central Iowa Recovery Inc.		Psychotherapeutic Treatme	41500	04042	366	62			5687.85
7413 V	1361	Central Iowa Recovery Inc.		Psychotherapeutic Treatme	41500	04242	366	62			1722.15
7413 V	1361	Central Iowa Recovery Inc.		Psychotherapeutic Treatme	41500	04042	366	62			5592.00
7413 V	1361	Central Iowa Recovery Inc.		Psychotherapeutic Treatme	41500	04042	397	62			1640.52
7413 V	1361	Central Iowa Recovery Inc.		Support Services - Suppor	41500	04332	329	62			83.70
7413 V	1361	Central Iowa Recovery Inc.		Day Habilitation	41500	04350	367	62			1204.16
				Disbursement# 5383		Disbursement Total					23,340.38
7442 V	7474	Century Link		Direct Admin - Telecommun	41500	04411	414	62			137.62
				Disbursement# 5384		Disbursement Total					137.62
7451 V	72467	Cherokee County Sheriff's Dept		Commitment - Sheriff Tran	41500	04074	353	62			38.00
				Disbursement# 5385		Disbursement Total					38.00
7453 V	82883	Christian Opportunity Center		Support Services - Suppor	41500	04232	329	62			416.82
7453 V	82883	Christian Opportunity Center		Day Habilitation	41500	04250	367	62			631.98
7453 V	82883	Christian Opportunity Center		Voc/Day - Individual Supp	41500	04250	368	62			748.84
7453 V	82883	Christian Opportunity Center		Day Habilitation	41500	04750	367	62			351.10
				Disbursement# 5386		Disbursement Total					2,148.74
7456 V	83451	Community Care of Knoxville		Comm Based Settings (6+ B	41500	04064	314	62			1952.69
				Disbursement# 5387		Disbursement Total					1,952.69

Disbursement Date 06/14/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
7403 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7403 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			40.00
7403 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7403 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7403 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7403 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
7403 V	276	Community Health Center of		Mental Health Services in	41500	04046	305	62			20.00
				Disbursement# 5388		Disbursement Total					160.00
7415 V	1751	Jessica Crawford		Services Management - Mil	41500	04022	413	62			102.83
7415 V	1751	Jessica Crawford		Services Management - Mil	41500	04222	413	62			99.81
7415 V	1751	Jessica Crawford		Services Management - Mil	41500	04322	413	62			99.81
				Disbursement# 5389		Disbursement Total					302.45
7454 V	83176	Diana Dawley		Direct Admin - Mileage &	41500	04411	413	62			89.51
				Disbursement# 5390		Disbursement Total					89.51
7417 V	2050	Dubuque County Sheriff		Commitment - Sheriff Tran	41500	04074	353	62			52.00
				Disbursement# 5391		Disbursement Total					52.00
7420 V	2243	Kathy Erickson		Mental Health Advocate -	41500	04075	413	62			133.38
				Disbursement# 5392		Disbursement Total					133.38
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			870.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2900.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2900.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2030.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2030.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			3190.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2320.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2030.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			580.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1160.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			870.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2320.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2320.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1160.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00

Disbursement Date 06/14/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			2610.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Evaluation	41500	04044	301	62			1740.00
7419 V	2219	eVizzit of Ia Psychiatry, JAIL		Crisis Stabilization Comm	41500	04044	312	62			900.00
				Disbursement# 5393		Disbursement Total					62,380.00
7436 V	5696	Eyerly Ball CMHS		Justice System Involved C	41500	04025	376	62			7138.00
				Disbursement# 5394		Disbursement Total					7,138.00
7421 V	2326	FIA Friendship Club, Inc.		Psychotherapeutic Treatme	41500	04042	366	62			2452.35
7421 V	2326	FIA Friendship Club, Inc.		Psychotherapeutic Treatme	41500	04242	366	62			3397.95
7421 V	2326	FIA Friendship Club, Inc.		Psychotherapeutic Treatme	41500	04342	366	62			413.70
				Disbursement# 5395		Disbursement Total					6,264.00
7423 V	2438	Foundation 2, Inc.		Mobile Response	41500	04044	307	62			9132.00
				Disbursement# 5396		Disbursement Total					9,132.00
7449 V	72119	Franklin County Sheriff's Off.		Commitment - Sheriff Tran	41500	04074	353	62			72.87
7449 V	72119	Franklin County Sheriff's Off.		Commitment - Sheriff Tran	41500	04074	353	62			58.67
				Disbursement# 5397		Disbursement Total					131.54
7422 V	2430	Freedom Pointe of Greater		Psychotherapeutic Treatme	41500	04042	366	62			7125.00
				Disbursement# 5398		Disbursement Total					7,125.00
7441 V	7342	GateHouse-DB Iowa Holdings		Direct Admin - Publicatio	41500	04411	400	62			211.04
7441 V	7342	GateHouse-DB Iowa Holdings		Direct Admin - Publicatio	41500	04411	400	62			172.34
				Disbursement# 5399		Disbursement Total					383.38
7424 V	2654	Kent L. Geffe		Commitment - Legal Repres	41500	04074	393	62			292.50
7424 V	2654	Kent L. Geffe		Commitment - Legal Repres	41500	04074	393	62			273.00
7424 V	2654	Kent L. Geffe		Commitment - Legal Repres	41500	04074	393	62			143.00
7424 V	2654	Kent L. Geffe		Commitment - Legal Repres	41500	04074	393	62			169.00
7424 V	2654	Kent L. Geffe		Commitment - Legal Repres	41500	04074	393	62			71.50
7424 V	2654	Kent L. Geffe		Commitment - Legal Repres	41500	04074	393	62			71.50
				Disbursement# 5400		Disbursement Total					1,020.50
7430 V	4293	Grundy County Sheriff's Office		Commitment - Sheriff Tran	41500	04074	353	62			102.22
				Disbursement# 5401		Disbursement Total					102.22
7425 V	2724	Hamilton County		Commitment - Sheriff Tran	41500	04074	353	62			69.00
7425 V	2724	Hamilton County		Commitment - Sheriff Tran	41500	04074	353	62			32.00
7425 V	2724	Hamilton County		Commitment - Sheriff Tran	41500	04074	353	62			32.00
				Disbursement# 5402		Disbursement Total					133.00
7426 V	2726	Hamilton County Jail		Prescription Medication (	41500	04046	306	62			91.37
				Disbursement# 5403		Disbursement Total					91.37
7427 V	2738	Hancock County Sheriff		Commitment - Sheriff Tran	41500	04074	353	62			41.70
				Disbursement# 5404		Disbursement Total					41.70

```
 Disbursement Date 06/14/2022

 Claim #   Vendor# Payee Name                        Invoice#  Description              Fund     Funct   Obj Dpt Prj Sub Line Amount

    7455 V   83215 Carrie Hisler                               Services Management - Mil 41500   04022   413  62                 111.30
    7455 V   83215 Carrie Hisler                               Services Management - Mil 41500   04222   413  62                 110.90
    7455 V   83215 Carrie Hisler                               Services Management - Mil 41500   04322   413  62                 108.03
                                                                     Disbursement#    5405       Disbursement Total              330.23

    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 288.99
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                  88.54
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 311.62
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 757.78
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 223.08
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 223.08
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 223.08
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 223.08
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 223.08
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 223.08
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 288.99
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 288.99
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 288.99
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 577.98
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 288.99
    7428 V    3532 Integrated Telehealth Partners              Mental Health Services in 41500   04046   305  62                 288.99
                                                                     Disbursement#    5406       Disbursement Total            4,808.34

    7429 V    3620 Jasper County Sheriff                       Commitment - Sheriff Tran 41500   04074   353  62                1070.65
    7429 V    3620 Jasper County Sheriff                       Commitment - Sheriff Tran 41500   04074   353  62                 268.29
    7429 V    3620 Jasper County Sheriff                       Prescription Medication ( 41500   04046   306  62                 445.19
    7429 V    3620 Jasper County Sheriff                       Commitment - Sheriff Tran 41500   04074   353  62                  24.20
    7429 V    3620 Jasper County Sheriff                       Commitment - Sheriff Tran 41500   04074   353  62                  68.35
                                                                     Disbursement#    5407       Disbursement Total            1,876.68

    7408 V    1158 Jefferson Telecom                           Services Management - Tel 41500   04022   414  62                  55.90
                                                                     Disbursement#    5408       Disbursement Total               55.90

    7410 V    1279 LifeWorks Community Services                Support Services - Suppor 41500   04032   329  62                6642.00
    7410 V    1279 LifeWorks Community Services                Day Habilitation          41500   04250   367  62                 782.40
    7410 V    1279 LifeWorks Community Services                Voc/Day - Individual Supp 41500   04250   368  62                 747.79
    7410 V    1279 LifeWorks Community Services                Support Services - Suppor 41500   04332   329  62                 105.71
    7410 V    1279 LifeWorks Community Services                Day Habilitation          41500   04350   367  62                 868.68
    7410 V    1279 LifeWorks Community Services                Voc/Day - Individual Supp 41500   04350   368  62                 374.42
    7410 V    1279 LifeWorks Community Services                Voc/Day - Group Supported 41500   04350   369  62                 417.48
    7410 V    1279 LifeWorks Community Services                Day Habilitation          41500   04750   367  62                 182.88
                                                                     Disbursement#    5409       Disbursement Total           10,121.36

    7448 V    8100 Marco                                       Direct Admin - Office Equ 41500   04411   636  62                 219.48
                                                                     Disbursement#    5410       Disbursement Total              219.48

    7431 V    4443 Marshall County                             Commitment - Sheriff Tran 41500   04074   353  62                  31.00
    7431 V    4443 Marshall County                             Commitment - Sheriff Tran 41500   04074   353  62                  86.00
    7431 V    4443 Marshall County                             Commitment - Sheriff Tran 41500   04074   353  62                 118.00
    7431 V    4443 Marshall County                             Commitment - Sheriff Tran 41500   04074   353  62                  75.00
```

Disbursement Date 06/14/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
				Disbursement# 5411		Disbursement Total					310.00
7447 V	7953	Robin McKee		Services Management - Mil	41500	04022	413	62			103.01
7447 V	7953	Robin McKee		Services Management - Mil	41500	04222	413	62			80.12
7447 V	7953	Robin McKee		Services Management - Mil	41500	04322	413	62			80.12
				Disbursement# 5412		Disbursement Total					263.25
7432 V	4766	Mid-Iowa Triumph Recovery Ctr		Psychotherapeutic Treatme	41500	04042	366	62			6344.00
				Disbursement# 5413		Disbursement Total					6,344.00
7433 V	4919	MIW Inc.		Voc/Day - Individual Supp	41500	04050	368	62			374.42
7433 V	4919	MIW Inc.		Voc/Day - Prevocational S	41500	04250	362	62			309.30
7433 V	4919	MIW Inc.		Voc/Day - Prevocational S	41500	04350	362	62			360.85
7433 V	4919	MIW Inc.		Voc/Day - Individual Supp	41500	04350	368	62			70.07
				Disbursement# 5414		Disbursement Total					1,114.64
7434 V	5283	North Iowa Vocational Center		Voc/Day - Individual Supp	41500	04050	368	62			59.90
7434 V	5283	North Iowa Vocational Center		Support Services - Suppor	41500	04032	329	62			1189.98
7434 V	5283	North Iowa Vocational Center		Voc/Day - Individual Supp	41500	04050	368	62			299.53
7434 V	5283	North Iowa Vocational Center		Comm Based Settings (6+ B	41500	04064	314	62			436.76
7434 V	5283	North Iowa Vocational Center		Comm Based Settings (6+ B	41500	04064	329	62			4438.30
7434 V	5283	North Iowa Vocational Center		Support Services - Suppor	41500	04232	329	62			270.45
7434 V	5283	North Iowa Vocational Center		Voc/Day - Prevocational S	41500	04250	362	62			176.12
7434 V	5283	North Iowa Vocational Center		Day Habilitation	41500	04250	367	62			105.41
7434 V	5283	North Iowa Vocational Center		Voc/Day - Individual Supp	41500	04250	368	62			374.42
7434 V	5283	North Iowa Vocational Center		Support Services - Suppor	41500	04332	329	62			129.80
7434 V	5283	North Iowa Vocational Center		Day Habilitation	41500	04350	367	62			253.59
7434 V	5283	North Iowa Vocational Center		Voc/Day - Individual Supp	41500	04350	368	62			888.62
7434 V	5283	North Iowa Vocational Center		Voc/Day - Group Supported	41500	04350	369	62			408.66
				Disbursement# 5415		Disbursement Total					9,031.54
7435 V	5548	Bill Patten		Direct Admin - Mileage &	41500	04411	413	62			65.52
				Disbursement# 5416		Disbursement Total					65.52
7437 V	5754	Polk County Auditor		Commitment - Sheriff Tran	41500	04074	353	62			41.70
				Disbursement# 5417		Disbursement Total					41.70
7438 V	5815	Poweshiek Co Sherriff's Dept		Commitment - Sheriff Tran	41500	04074	353	62			56.74
7438 V	5815	Poweshiek Co Sherriff's Dept		Commitment - Sheriff Tran	41500	04074	353	62			57.74
				Disbursement# 5418		Disbursement Total					114.48
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			21.25
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			91.34
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			91.34
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			91.34
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			47.54
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			91.34
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			91.34
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			91.34
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			68.50

Disbursement Date 06/14/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line Amount
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			91.34
7452 V	82831	Prairie Ridge Integrated		Psychotherapeutic Treatme	41500	04042	305	62			68.50
				Disbursement# 5419		Disbursement Total					845.17
7439 V	5910	Quill Corporation		Direct Admin - Stationary	41500	04411	260	62			15.99
				Disbursement# 5420		Disbursement Total					15.99
7440 V	6096	Respite Connection		Support Services - Respit	41500	04332	325	62			573.60
				Disbursement# 5421		Disbursement Total					573.60
7404 V	322	Salvation Army		Support Services - Repres	41500	04032	327	62			672.00
7404 V	322	Salvation Army		Support Services - Repres	41500	04232	327	62			144.00
				Disbursement# 5422		Disbursement Total					816.00
7406 V	771	Sioux Rivers Region		Mental Health Advocate -	41500	04075	395	62			123.10
				Disbursement# 5423		Disbursement Total					123.10
7407 V	1091	Julie Smith		Public Education Services	41500	04005	373	62			201.24
				Disbursement# 5424		Disbursement Total					201.24
7443 V	7498	U.S. Cellular		Direct Admin - Telecommun	41500	04411	414	62			3.94
				Disbursement# 5425		Disbursement Total					3.94
7444 V	7601	VISA		Direct Admin - Educationa	41500	04411	422	62			115.00
7444 V	7601	VISA		Direct Admin - Publicatio	41500	04411	400	62			222.93
7444 V	7601	VISA		Direct Admin - Stationary	41500	04411	260	62			597.30
7444 V	7601	VISA		Direct Admin - Postage &	41500	04411	412	62			118.00
7444 V	7601	VISA		Direct Admin - Mileage &	41500	04411	413	62			19.61-
7444 V	7601	VISA		Direct Admin - Mileage &	41500	04411	413	62			168.00
7444 V	7601	VISA		Direct Admin - Informatio	41500	04411	632	62			736.66
				Disbursement# 5426		Disbursement Total					1,938.28
7445 V	7696	Webster County Sheriff		Commitment - Sheriff Tran	41500	04074	353	62			15.00
7445 V	7696	Webster County Sheriff		Commitment - Sheriff Tran	41500	04074	353	62			3.00
				Disbursement# 5427		Disbursement Total					18.00
7446 V	7806	Russell Wood		Direct Admin - Mileage &	41500	04411	413	62			888.73
				Disbursement# 5428		Disbursement Total					888.73
7405 V	350	Woolstock Mutal Telephone Assn		Direct Admin - Telecommun	41500	04411	414	62			55.00
				Disbursement# 5429		Disbursement Total					55.00

58	Total Disbursements	221,715.16
0	Total ACH	.00
0	Total EFT	.00
58	Grand Total	221,715.16
	Credits/Refunds Included	19.61

Disbursement Date 06/14/2022

Claim #	Vendor#	Payee Name	Invoice#	Description	Fund	Funct	Obj	Dpt	Prj	Sub	Line	Amount

Totals by Fund

41500	Central Iowa Community Service	221,715.16
	Final Total	221,715.16

End of report

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Pillar of Cedar Valley

Chart of Account	Service Description	Unit of Service	Rate
64317	Nursing Facility ICF/PMI	Daily	$278.27

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Funding for all contracted services requires prior authorization and individuals shall meet Pre-Admission Screening and Resident Review (PASRR) level of care and CICS Management Plan criteria. CICS will issue a Notice of Decision to the client and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Clients are responsible to pay all copayment amounts directly to the provider.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Pillar of Cedar Valley:

By: _____

Print Name: Hilary Schmidt

Print Title: administrator

Date: 5/26/22

Central Iowa Community Services
Provider and Program Participation Agreement

THIS PROVIDER AND PROGRAM PARTICIPATION AGREEMENT ("**Agreement**"), entered into this First day of July, 2022, is by and between Central Iowa Community Services ("**CICS**") and North Iowa Transitional and Employment Services Inc. dba 43 North Iowa ("**Provider**").

RECITALS:

A. CICS is a governmental entity organized under Chapter 28E of the Code of Iowa, governed by its Governing Board. Mental health and disability services are funded and administered by CICS within the scope and according to the criteria of the Regional Management Plan. CICS desires to contract with Provider to provide Covered Services for the benefit of CICS Individuals.

B. Provider is licensed, certified and/or accredited under the laws of the State of Iowa to provide mental health, intellectual disabilities, and/or developmental disability services and desires to contract with CICS to provide Covered Services for the benefit of CICS Individuals.

C. An effective service delivery environment should be based on individualized, person centered, strengths-based practices which are trauma informed, co-occurring capable, and culturally competent.

In consideration of the premises and promises contained herein, it is mutually agreed by and between CICS and Provider as follows:

SECTION 1
Definitions

Administrative Team: Community Service Directors of Region member counties.

CICS Governing Board: The board of CICS responsible for governing CICS.

CICS Individual: A person who is eligible and authorized to receive funding as defined in the Regional Management Plan as approved by the Director of the Department of Human Services, State of Iowa.

Co-payment: The amount that may be charged to CICS Individual at the time services are rendered.

Covered Services: Services enumerated in the Regional Management Plan, as approved by the Director of the Department of Human Services, State of Iowa.

HIPAA: Collectively, the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and all implementing regulations.

Individual Authorization: An Individual Authorization is a standard form, signed by an individual, to allow disclosure of the individual's Protected Health Information. The form must comply with HIPAA and all other applicable federal and state laws. The individual may revoke the Individual Authorization at any time in accordance with its terms.

Protected Health Information: Individually identifiable health information that is transmitted by or maintained in electronic media or transmitted by or maintained in any other form or medium.

Region: The inter-governmental entity created under Chapter 28E of the Code of Iowa and Section 331.390 of the Code of Iowa that includes member counties of CICS.

Regional Management Plan: CICS' plan, developed pursuant to Iowa Code Section 331.393, for providing an array of cost-effective individualized services and supports that assist CICS Individuals in the Region to be as independent, productive, and integrated into the community as possible, within the constraints of the services fund.

SECTION 2
Duties of Provider

Section 2.1 Provision of Covered Services. Provider shall provide Covered Services to each CICS Individual who is authorized by the Administrative Team or Administrative Team designee ("**Designee**") to receive such services to the extent designated in Attachment A, Service Definitions and Rates. Such services shall be rendered in compliance with applicable laws and regulations and the Regional Management Plan. Provider shall provide Covered Services in a manner that: (a) documents the services provided, in conformance with applicable federal, state and local laws and regulations and the Regional Management Plan, and (b) protects the confidentiality of the CICS Individual's medical records, including, without limitation, any Protected Health Information. Provider may decline providing services to a CICS Individual provided that Provider communicates this decision to Administrative Team or Designee within twenty-four (24) hours of declining such services.

Section 2.2 Compliance with the Regional Management Plan. Provider and its staff shall be bound by and provide Covered Services in compliance with the Regional Management Plan. Failure to comply with the Regional Management Plan may result in sanctions including, without limitation, the loss of reimbursement and/or termination of the Agreement. If Provider does not agree with the sanction, Provider may appeal such action to the CICS Governing Board. The decision of the CICS Governing Board shall be final and conclusive and non-appealable.

Section 2.3 Authorization and Notification Requirements. All Covered Services provided to CICS Individuals by Provider must be authorized by CICS prior to or at the time of rendering services or in accordance with the Regional Management Plan. The Regional Management Plan shall not diminish Provider's obligation to render Covered Services consistent with the applicable

standard of care. Provider shall be required to obtain from each CICS Individual an Individual Authorization that allows Provider to disclose any information about the Individual to CICS.

Section 2.4 Access to Books and Records. Unless otherwise required by applicable statutes or regulation, Provider shall allow CICS access to books, records, or cost reports as needed to establish rates or for purposes of appeals, utilization, grievance, claims payment review, individual medical records review, or financial audits, during the term of this Agreement and seven (7) years following its termination. Provider shall obtain any necessary Individual Authorization to allow CICS to exercise its rights under this Agreement.

Section 2.5 Licenses. At all times, Provider and the providers it employs or contracts with to provide services to CICS Individuals shall have all necessary licenses and certifications to perform the Covered Services.

Section 2.6 Major Incident Reporting. To the extent Provider is otherwise required to comply with Iowa Administrative Code ("IAC") Chapter 77, Provider shall promptly notify CICS in writing when a "major incident" as defined in IAC 441-77 involves a CICS Individual and the major incident would otherwise be required to be reported if the CICS Individual were receiving a Medicaid funded service. Provider may use the CICS Major Incident Report Form or Iowa Medicaid Critical Incident Report form for purposes of the notification.

SECTION 3
Service Delivery and Assessment

Section 3.1 Service Delivery. The Region encourages the use of Evidence Based Practices, Research Based Practices and Promising Practices in service delivery.

Section 3.2 Service Assessment. The Region is charged with the responsibility of collecting Outcome measurement information. Provider is required to follow the reporting requirements for any outcome measures listed in Attachment A. If the Region implements additional measures, this contract will be amended to reflect said changes.

Section 3.3 Incentives. Provider may qualify for incentive payments if it meets reporting and outcome participation requirements established by CICS.

SECTION 4
Claims Submission and Payment

Section 4.1 Claims Submission. Provider agrees to submit all claims for Covered Services in accordance with the Regional Management Plan.

Section 4.2 Claims Payment. CICS will pay claims for Covered Services in accordance with the Regional Management Plan.

Section 4.3 Compensation to Provider. Provider agrees to accept payment from CICS for Covered Services provided to CICS Individuals under this Agreement as payment in full, less any Co-payment or other amount that is due from CICS Individuals for such services. Provider shall not negotiate and/or accept lower rates or more favorable terms than those provided for in this Agreement from any other Region or county. Rates of compensation for Covered Services are set forth in Attachment A, Service Definitions and Rates.

SECTION 5
Relationship Between the Parties

Section 5.1 Relationship Between CICS and Provider. The relationship between CICS and Provider is solely that of independent contractors and nothing in this Agreement shall be construed or deemed to create any other relationship including one of employment, agency, or joint venture. Provider shall maintain social security, workers' compensation and all other employee benefits covering Provider's employees as required by law.

SECTION 6
Liability Insurance

Section 6.1 Provider Hold Harmless and Indemnification. Provider shall defend, hold harmless and indemnify CICS against any and all claims, liability, damages, judgments, and expenses, including, without limitation, reasonable attorney fees and costs, asserted against, imposed or incurred by CICS that arise out of acts or omissions of Provider or Provider's employees, agents or representatives in the discharge of Provider's responsibilities under this Agreement.

Section 6.2 Provider Liability Insurance. Provider agrees to carry comprehensive general liability insurance (claims-made with appropriate tail coverage or occurrence-based), at its own expense, in an amount of not less than $1,000,000 per occurrence and $2,000,000 aggregate. If Provider employs professionally licensed individuals, Provider also agrees to carry professional liability insurance (claims-made with appropriate tail coverage or occurrence-based), at its own expense, in an amount of not less than $1,000,000 per occurrence. Both types of coverages shall cover any claims with respect to Covered Services that may arise out of an incident occurring during the term of this Agreement as well as any claims in connection with the performance of Provider's responsibilities under this Agreement. Provider shall furnish to CICS on an annual basis proof of each required insurance, which proof will include the name of the carrier(s), effective dates of each coverage and coverage amounts.

SECTION 7
Laws and Regulations

Section 7.1 Laws and Regulations. Provider represents, covenants, and warrants that it is, and during the term of this Agreement will continue to be, operating in full compliance with all applicable federal and state laws.

Section 7.2 Compliance with Civil Rights Laws. Provider agrees not to discriminate or differentiate in the treatment of any individual based on age, race, creed, color, sex, sexual orientation, gender identity, national origin, religion, or disability. Provider agrees to ensure mental health and disability services are rendered to CICS Individuals in the same manner, and in accordance with the same standards and with the same availability, as offered to any other individual receiving services from Provider.

Section 7.3 Equal Opportunity Employer. CICS counties are equal employment opportunity employers. CICS supports a policy which prohibits discrimination against any employee or applicant for employment on the basis of age, race, sex, creed, color, sex, sexual orientation, gender identity, national origin, religion, or disability, or any other classification protected by law or ordinance. Provider agrees that it is in full compliance with this policy.

Section 7.4 Confidentiality of Records. CICS and Provider agree to maintain the confidentiality of all information regarding Covered Services provided to CICS Individuals under this Agreement in accordance with any applicable laws and regulations, including, without limitation, HIPAA. Provider acknowledges that in receiving, storing, processing, or otherwise dealing with information from CICS about CICS Individuals, it is fully bound by federal and state laws and regulations, including, without limitation, HIPAA, governing the confidentiality of medical records, mental health and disability services records, and Protected Health Information.

SECTION 8
Term and Termination

Section 8.1 Term. The term of this Agreement shall be for a period of eighteen (18) months commencing on the date first above written through December 2023.

Section 8.2 Termination Without Cause. Either party may terminate this Agreement without cause upon sixty (60) days prior written notice of termination to the other party.

Section 8.3 Termination With Cause by CICS. CICS shall have the right to terminate this Agreement immediately by giving written notice to Provider upon the occurrence of any of the following events: (a) restriction, suspension or revocation of Provider's license, certification or accreditation or the license of any provider employed by or contracted with Provider to perform services under this Agreement; (b) Provider's loss of any liability insurance required under this Agreement; or (c) bankruptcy filing by the Provider.

Section 8.4 Termination by Provider. Provider may terminate this Agreement pursuant to Section 9.2 or 9.3; provided that Provider notifies CICS within thirty (30) days of the effective date of such amendment of its disagreement with such amendment.

Section 8.5 Termination for Breach. Either party shall have the right to terminate this Agreement for material breach of this Agreement by the other party that is not cured within thirty (30) days after written notice to the other party is provided.

Section 8.6 Information to CICS Individuals. Provider acknowledges the right of CICS to inform CICS Individuals of Provider's termination of this Agreement and agrees to cooperate with CICS in deciding on the form of such notification.

Section 8.7 Continuation of Services After Termination. Upon request by CICS for up to sixty (60) days upon termination notification, Provider shall continue to render Covered Services in accordance with this Agreement until CICS has transferred CICS Individuals to another provider or until such CICS Individual(s) are discharged.

Section 8.8 Notices to CICS. Any notice, request, demand, waiver, consent, approval or other communication to CICS which is required or permitted herein shall be in writing and shall be deemed given only if delivered personally, or sent by registered mail or certified mail, or by express mail courier service, postage prepaid, as follows:

CICS Operations Officer
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010

Section 8.9 Notices to Provider. Any notice, request, demand, waiver, consent, approval or other communication to Provider which is required or permitted herein shall be in writing and shall be deemed given only if delivered personally, or sent by registered mail or certified mail, or by express mail courier service, postage prepaid, as follows:

43 North Iowa
Attention: John Derryberry
111 2nd St NE
Mason City, IA 50401

SECTION 9
Amendments

Section 9.1 Amendment. Subject to Sections 9.1 and 9.2, this Agreement may be amended at any time only by the mutual written agreement of the parties.

Section 9.2 Regulatory Amendment. CICS may amend this Agreement to comply with applicable statutes and regulations and shall give written notice to Provider of such amendment and its effective date. Such amendment will not require sixty (60) days advance written notice. If the Provider does not agree with the amendment, Provider may terminate this Agreement as provided in Section 8.4.

Section 9.3 Regional Management Plan Amendment. CICS may also amend this Agreement to comply with changes in the Regional Management Plan and shall give written notice to Provider of such amendment and its effective date. Such amendment will not require sixty (60) days advance written notice. If Provider does not agree with the Amendment, Provider may terminate this Agreement as provided in Section 8.4.

SECTION 10
Other Terms and Conditions

Section 10.1 Non-Exclusivity. This Agreement does not confer upon the Provider any exclusive right to provide services to CICS Individuals in Provider's geographical area. CICS reserves the right to contract with other providers. The parties agree that Provider may continue to contract with other organizations.

Section 10.2 Assignment. Provider may not assign any of its rights and responsibilities under this Agreement to any person or entity without the prior written approval of CICS. Any assignment not in accordance with this Section 10.2 shall be null and void.

Section 10.3 Subcontracting. Provider may not subcontract any of its rights and responsibilities under this Agreement to any person or entity without prior notification to CICS. Mutual agreement must be obtained between Provider, CICS, and any subcontractor.

Section 10.4 Entire Agreement and Amendments. This Agreement and its attachments constitute the entire agreement between CICS and Provider and supersedes or replaces any prior agreements between CICS and Provider relating to its subject matter. This Agreement may be amended only pursuant to a written document executed by both parties.

Section 10.5 Rights of Provider and CICS. Provider agrees that CICS may use Provider's name, address, telephone number, description of Provider, and Provider's care and specialty services in any promotional activities. Otherwise, Provider and CICS shall not use each other's name, symbol or service mark without prior written approval of the other party.

Section 10.6 Invalidity. If any term, provision or condition of this Agreement shall be determined invalid by a court of law, such invalidity shall in no way affect the validity of any other term, provision or condition of this Agreement, and the remainder of the Agreement shall survive in full force and effect unless to do so would substantially impair the rights and obligations of the parties to this Agreement.

Section 10.7 No Waiver. The waiver by either party of a breach or violation of any provisions of this Agreement shall not operate as or be construed to be a waiver of any subsequent breach.

Section 10.8 Execution. This Agreement has been executed by the parties hereto, through their duly authorized officials.

Section 10.9 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Iowa (but without regard to provisions thereof relating to conflicts of laws).

Section 10.10 No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein made confer, upon any person other than the parties to this Agreement and their respective successors or assigns of the parties, any rights, remedies, obligations or liabilities whatsoever.

Section 10.11 Survival. Sections 2.4, 6.1, 6.2, 8.6, 8.8, 8.9, and Section 10 shall survive any termination of this Agreement.

Section 10.12 Waiver of Jury Trial. EACH PARTY HEREBY UNCONDITIONALLY WAIVES ANY RIGHT TO A JURY TRIAL WITH RESPECT TO AND IN ANY ACTION, PROCEEDING, CLAIM, COUNTERCLAIM, DEMAND OR OTHER MATTER WHATSOEVER ARISING OUT OF THIS AGREEMENT.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

North Iowa Transitional and Employment Services Inc. dba 43 North Iowa:

By: _____

Print Name: John Berryberry

Print Title: Executive Director

Date: 6/13/23

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
North Iowa Transitional and Employment Services Inc. dba 43 North Iowa

Chart of Account	Service Description	Unit of Service	Rate
42329	Intensive Residential Service Remodel Startup Costs	N/A	Maximum of $361,100.00
42329	Intensive Residential Service Startup Service Costs	N/A	Maximum of $66,526.00
42329	Intensive Residential Service	Daily	$536.50

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Remodel Startup Costs

Provider and CICS will agree upon a remodel timeline, upon agreement of this, Provider will submit to CICS an invoice for 50% of the Intensive Residential Service Remodel Startup Cost ($180,550.00). After expending the initial remodel startup funding, Provider will invoice CICS for reimbursement of remaining remodel costs not to exceed a total maximum of $361,100.00. Provider will submit documentation verifying remodel expenses CICS funds are used and reimbursed for.

Within 45 days of remodel completion, Provider will submit to CICS an Actual Cost Report for remodel costs, CICS and Provider will then cost settle on the remodel costs.

Service Startup Costs

Provider will invoice CICS Service Startup Costs of $66,526.00 between 30 and 60 days prior to implementing Intensive Residential Services. Provider will submit documentation of service startup expenses to CICS. This amount will be included in the cost settlement identified below for FY23.

Intensive Residential Service

Funding for Intensive Residential Service requires prior authorization and individuals shall meet CICS Management Plan criteria. CICS will issue a Notice of Decision to the client and Provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Clients are responsible to pay all copayment amounts directly to the provider.

CICS will fund up to four unfunded beds per day. Provider will bill CICS by the 15th of the month following service delivery.

By August 15, 2023, Provider will submit an Actual Cost Report for Intensive Residential Service costs for FY23. CICS and Provider will then cost settle on service costs.

By February 15, 2024, Provider will submit an Actual Cost Report for Intensive Residential Service costs for July 1, 2023 – December 30, 2023. CICS and Provider will cost settle on service costs for this timeframe.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

North Iowa Transitional and Employment Services Inc. dba 43 North Iowa:

By: _____

Print Name: John Derryberry

Print Title: Executive Director

Date: 6/13/22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Arc of Marshall County

Chart of Account	Service Description	Unit of Service	Rate
42366	Special Recreation	Monthly	$628.00/month

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

At time of monthly billing submission, provider will submit documentation of participant names for month billed.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Arc of Marshall County:

By: Allen Fagerlund

Print Name: ALLEN FAGERLUND

Print Title: EXEC. DIRECTOR

Date: 6-5-2022

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Boone County

Chart of Account	Service Description	Unit of Service	Rate
75XXX	Mental Health Advocate	Monthly	See Other Terms

OTHER TERMS:
CICS will reimburse for Boone County Mental Health Advocate expenses. Mental Health Advocate services are provided and funded for Boone, Greene, Madison, Warren, and Poweshiek Counties. At the time of monthly billing, Mental Health Advocate will submit names of individuals served for the month of service.

Central Iowa Community Services:

By: _____

Print Name: _____

Print Title: Chair, CICS Governing Board

Date: _____

Boone County:

By: _____

Print Name: _____

Print Title: _____

Date: _____

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Capstone Behavioral Healthcare

Chart of Account	Service Description	Unit of Service	Rate
46305 Jail 42305 Outpatient	Therapy Evaluation (90791)	Visit	$155.61
46305 Jail 42305 Outpatient	Therapy 90837 90834 90832	 60 Min. 45 Min. 30 Min.	 $114.17 $114.17 $59.43
46305 Jail 42305 Outpatient	Group Therapy (90853)	Hour	$69.43
46305 Jail 42306 Outpatient	Psychiatric Evaluation (90792)	Visit	Dr. $300.67 ARNP $232.09 PA $232.09
46305 Jail 42306 Outpatient	Medication Management (99213)	15 Min.	Dr. $101.60 ARNP $72.45 PA $72.45
42306	Care Coordination	One tele health session	$31.21
42305	Family Therapy (90846)	Hour	$98.83
41305	Injection (96372)	N/A	$26.38
41305	Nursing (S9123)	Nurse Visit	$58.64
43301	Assessment, Evaluation, & Early Identification	Hour	$190.89
42305	Licensed Independent Social Work (LISW) Onboarding & Access July 2022-June 2023 (Morgan Bloom, LISW)*	N/A	Maximum $10,000.00
42306	Medication Prescribing & Management Onboarding & Access July 2022-June 2023 (Laura Owens, ARNP)**	N/A	Maximum $15,000.00
44301	Crisis Therapy Services (2 appointments/month – Jasper) (1 appointment/month – Poweshiek)	60 Min. 45 Min. 30 Min.	$114.17 $114.17 $59.43
44301	Crisis Psychiatric Evaluation (2 appointments/month – Jasper) (1 appointment/month – Poweshiek)	Visit	Dr. $300.67 ARNP $232.09 PA $232.09

44305	Community Based Crisis Intervention Services	Hour	$126.00
05373	Public Education, Prevention and Education	Hour	$126.00; Maximum of 12 hours/contract period
32329	Supported Community Living – Home Based Habilitation High Recovery Recovery Transitional Medium Need Intensive I Intensive II Intensive III	 UA; .25-2 Hours/Day UB; 2.25-4 Hours/Day UC; 4.25-8.75 Hours/Day UD; 9-12.75 Hours/Day U8; 13-16.75 Hours/Day U9; 17-24 Hours/Day	 $54.09 $116.72 $135.28 $218.38 $221.40 $388.73
42396	Community Support Services– Poweshiek Co. Low level CSS High level CSS	 Monthly Monthly	 $176.87 $520.20
42366	Clubhouse - Poweshiek Co.	Monthly	$7,263.00
42366	Drop-in Center – Jasper Co.	Monthly	$7,757.00
25376	Justice Coordination/ Jail Diversion	Monthly	$6,608.00

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Psychological Testing is a service under Assessment, Evaluation, & Early Identification.

CICS may be billed the Crisis Psychiatric Evaluation rate if the Crisis Psychiatric Evaluation appointment is reserved and unfilled. Two Crisis Psychiatric Evaluation appointments shall be available monthly for Jasper County and one per month for Poweshiek County. If crisis medication management is needed, this can be performed during the reserved crisis psychiatric evaluation time slot and billable at the contracted medication management reimbursement rate as applicable. CICS Service Coordination staff shall be informed of the reserved time slot for the Crisis Psychiatric Evaluation service.

CICS may be billed the Crisis Therapy Services 60-minute rate if the Crisis Therapy appointment is reserved and unfilled. Two Crisis Therapy appointments shall be available monthly for Jasper County and one per month for Poweshiek County. If a crisis therapy evaluation is needed, this can be performed during the reserved crisis therapy time slot and billable at the contracted therapy

evaluation reimbursement rate as applicable. CICS Service Coordination staff shall be informed of the reserved time slot for the Crisis Therapy Service.

*LISW will provide Outpatient Therapy Services to residents of CICS region and accept and provide services to patients with Medicaid and/or Medicare, private insurance, and MHDS regional funding. The LISW Onboarding & Access Fee shall be prorated and paid in the month of June 2023 for Fiscal Year 2023 with an invoice submitted by the provider.

If LISW is less than full-time and/or practices less than full-time in the Outpatient setting, the Access fee will be prorated based on the total number of hours LISW services are available to patients in the Outpatient setting.

In the event the LISW does not maintain employment with Capstone Behavioral Healthcare and upon initiation continue to provide Outpatient Therapy Services in the Outpatient setting for the entire CICS Provider and Program Participation Agreement service period ending June 30, 2023 no LISW Onboarding & Access fee will be paid by CICS.

** Psychiatric Prescriber will provide Outpatient Medication Prescribing and Management services to residents of CICS region and accept and provide services to patients with Medicaid and/or Medicare, private insurance, and MHDS regional funding. The Medication Prescribing & Management Onboarding & Access Fee shall be prorated and paid by June 30, 2023 for Fiscal Year 2023 with an invoice submitted by the provider.

If Psychiatric Prescriber is less than full-time and/or practices less than full-time in the Outpatient setting, the Access fee will be prorated based on the total number of hours Psychiatric Prescriber services are available to patients in the Outpatient setting.

In the event the Psychiatric Prescriber does not maintain employment with Capstone Behavioral Healthcare and upon initiation continue to provide Psychiatric Prescriber services in the Outpatient setting for the entire CICS Provider and Program Participation Agreement service period ending June 30, 2023 no Medication Prescribing & Management Onboarding & Access Fee will be paid by CICS.

Public Education, Prevention and Education Services - Education services means activities that increase awareness and understanding of the causes and nature of conditions or factors which affect an individual's development and functioning. Prevention means efforts to increase awareness and understanding of the causes and nature of conditions or situations which affect an individual's functioning in society. Prevention activities are designed to convey information about the cause of conditions, situations, or problems that interfere with an individual's functioning or ways in which that knowledge can be used to prevent their occurrence or reduce their effect, and may include but are not limited to, training events, webinars, presentations, and public meetings. Provider outreach activities and/or marketing activities would not fall under Public Education, Prevention and Education. Provider needs to seek written approval by CICS for funding of Public Education, Prevention and Education services.

Funding for outpatient services must be pre-authorized by CICS. CICS will issue a Notice of Decision to the patient and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Patients are responsible to pay all copayment amounts directly to the provider.

CICS funds may supplement patients with insurance any remaining amount due, up to the "allowed charge" on the insurance Explanation of Benefits (EOB) or the contracted CICS rate, whichever is less.

Based on the client's individualized assessment, CICS will honor the Provider's Medicaid tiered rate for Home Based Habilitation services. Documentation of the client's individualized assessment and the Medicaid tiered rate shall be provided to CICS by the Provider. If a current individualized client assessment is not available CICS will complete an assessment and work with the provider in identifying the applicable Medicaid tiered rate for the Individual. Individual rates may be reviewed at the request of CICS or the Provider as determined necessary.

For Clubhouse – Poweshiek County Drop-in Center services the monthly amount to be billed and reimbursed is not to exceed $7,263.00/month with all employee positions filled. If employee positions are unfilled at any time, provider needs to notify CICS to determine a monthly reimbursement up to the $7,263.00/month based on the budget provided for this Agreement. At time of monthly billing submission, provider will submit daily attendance log documentation and participant names for month billed.

For Drop-in Center – Jasper County $7,757.00 is the monthly amount to be billed/reimbursed for Drop In Center services when all employee positions are filled. If employee positions are unfilled at any time, provider needs to notify CICS to determine a monthly reimbursement up to the $7,757.00 based on the budget provided for this Agreement. At time of monthly billing submission, provider will submit daily attendance log documentation and participant names for month billed.

For billing of Justice Coordination/Jail Diversion, staff positions must provide service for the entire month or rate is to be prorated based on the budget provided for this Agreement. Monthly amount to be billed and reimbursed not to exceed $6,608.00/month. For individual client eligibility provider will seek funding prior authorization with CICS. At time of monthly billing submission for Justice Coordination/Jail Diversion services, provider will submit documentation of participant names with hours served for month billed.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Capstone Behavioral Healthcare:

By: Julie Smith

Print Name: Julie Smith

Print Title: Center Director

Date: 5-25-2022

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Center Associates

Chart of Account	Service Description	Unit of Service	Rate
46305 Jail 42305 Outpatient	Therapy Evaluation (90791)	Visit	$155.61
46305 Jail 42306 Outpatient	Psychiatric Evaluation (90792)	Visit	Dr. $300.67 ARNP $232.09 PA $232.09
46305 Jail 42305 Outpatient	Therapy 90837 90834 90832	 60 Min. 45 Min. 30 Min.	 $114.17 $114.17 $59.43
46305 Jail 42306 Outpatient	Medication Management (99213)	15 Min.	Dr. $101.60 ARNP $72.45 PA $72.45
42306 Outpatient	Care Coordination	One Tele Health Session	$31.21
46305 Jail 42305 Outpatient	Group Therapy (90853)	Hour	$69.43
42305	Family Therapy (90846)	Hour	$98.83
42305	Individual - Behavioral Health Intervention Services (BHIS)	15 Min.	$21.88
42305	Family – Behavioral Health Intervention Services (BHIS)	15 Min.	$21.43
41305	Injection (96372)	N/A	$26.38
41305	Nursing (S9123)	Nurse Visit	$58.64
43301	Assessment, Evaluation, & Early Identification	Hour	$190.89
44301	Crisis Therapy Services (2 appointments/week)	60 Min. 45 Min. 30 Min.	$114.17 $114.17 $59.43
44301	Crisis Psychiatric Evaluation (2 appointments/week)	Visit	Dr. $300.67 ARNP $232.09 PA $232.09
44305	Community Based Crisis Intervention Services	Hour	$126.00
05373	Public Education, Prevention and Education	Hour	$126.00; Maximum of 12 hours/contract period
25376	Justice Coordination/ Jail Diversion	Monthly	$7,260.00

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Psychological Testing is a service under Assessment, Evaluation, & Early Identification.

CICS may be billed the Crisis Psychiatric Evaluation rate if the Crisis Psychiatric Evaluation appointment is reserved and unfilled. Two Crisis Psychiatric Evaluation appointments shall be available weekly. If crisis medication management is needed, this can be performed during the reserved crisis psychiatric evaluation time slot and billable at the contracted medication management reimbursement rate as applicable. CICS Service Coordination staff shall be informed of the reserved time slots for the Crisis Psychiatric Evaluation service.

CICS may be billed the Crisis Therapy Services 60-minute rate if the Crisis Therapy appointment is reserved and unfilled. Two Crisis Therapy appointments shall be available weekly. If a crisis therapy evaluation is needed, this can be performed during the reserved crisis therapy time slot and billable at the contracted therapy evaluation reimbursement rate as applicable. CICS Service Coordination staff shall be informed of the reserved time slots for the Crisis Therapy Service.

Public Education, Prevention and Education Services - Education services means activities that increase awareness and understanding of the causes and nature of conditions or factors which affect an individual's development and functioning. Prevention means efforts to increase awareness and understanding of the causes and nature of conditions or situations which affect an individual's functioning in society. Prevention activities are designed to convey information about the cause of conditions, situations, or problems that interfere with an individual's functioning or ways in which that knowledge can be used to prevent their occurrence or reduce their effect, and may include but are not limited to, training events, webinars, presentations, and public meetings. Provider outreach activities and/or marketing activities would not fall under Public Education, Prevention and Education. Provider needs to seek written approval by CICS for funding of Public Education, Prevention and Education services.

Funding for outpatient services must be pre-authorized by CICS. CICS will issue a Notice of Decision to the patient and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Patients are responsible to pay all copayment amounts directly to the provider. CICS funds may supplement patients with insurance any remaining amount due, up to the "allowed charge" on the insurance Explanation of Benefits (EOB) or the contracted CICS rate, whichever is less.

Combined funding for Individual and Family BHIS shall not exceed 192 units for a 6 month funding authorization period. Units will be prorated for shorter funding authorization periods.

For billing of Justice Coordination/Jail Diversion, position must provide service for the entire month or rate is to be prorated. Monthly amount to be billed and reimbursed not to exceed $7,260.00/month. For individual client eligibility provider will seek funding prior authorization with CICS. At time of monthly billing submission for Justice Coordination/Jail Diversion services, provider will submit documentation of participant names with hours served for month billed.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Center Associates:

By: _____

Print Name: PAUL DANIEL

Print Title: CEO

Date: 6/13/2022

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Central Iowa Juvenile Detention Center

Chart of Account	Service Description	Unit of Service	Rate
74353	Civil Commitment Transportation – First Person (Driver)	Hour	$57.96
74353	Civil Commitment Transportation – Second Person	Hour	$30.09
31354	General Transportation – First Person (Driver)	Hour	$57.96
31354	General Transportation – Second Person	Hour	$30.09

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

For Civil Commitment Transport – 100% secure vehicle, minimum of 98%, used to transport from Emergency Room.

Reimbursable expense is round trip from point of origination of the transport driver to client destination(s) and return to point of origination of transport driver.

Prior authorization is not required for Civil Commitment transportation and for transportation from an Emergency Department to a voluntary Inpatient Behavioral Health Hospitalization.

Prior authorization is not required for General Transportation for transport to an Access Center, Subacute service or Crisis Stabilization service when admission is from a hospital or physician office. Prior authorization is also not required for return trip to the county the client was admitted to the Access Center, Subacute, or Crisis Stabilization service from if no other transportation or funding is available.

General Transportation for all other purposes must be prior authorized by CICS including transportation from an Inpatient Behavioral Health Hospitalization.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Central Iowa Juvenile Detention Center:

By: Tony D Reed

Print Name: Tony J. Reed

Print Title: Executive Director

Date: 5-25-22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Central Iowa Psychological Services

Chart of Account	Service Description	Unit of Service	Rate
46305 Jail 42305 Outpatient	Therapy Evaluation (90791)	Visit	$155.61
46305 Jail 42305 Outpatient	Therapy 90837 90834	 60 Min. 45 Min.	 $114.17 $114.17
46305 Jail 42305 Outpatient	Therapy 90832	 30 Min.	 $59.43
46305 Jail 42305 Outpatient	Group Therapy (90853)	Hour	$69.43
42305 Outpatient	Family Therapy (90846)	Hour	$98.83
43301 Outpatient	Evaluation, Non-Crisis Assessment and Evaluation	Hour	$190.89
42306 Outpatient	Psychiatric Evaluation (90792)	Visit	Dr $300.67 ARNP $232.09 PA $232.09
42306 Outpatient	Medication Management (99213)	15 Min.	Dr. $101.60 ARNP $72.45 PA $72.45

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Funding for all contracted services must be pre-authorized by CICS. CICS will issue a Notice of Decision to the patient and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Patients are responsible to pay all copayment amounts directly to the provider. CICS funds may supplement patients with insurance any remaining amount due, up to the "allowed charge" on the insurance Explanation of Benefits (EOB) or the contracted CICS rate, whichever is less.

Psychological Testing is a service under Evaluation, Non-Crisis Assessment and Evaluation.

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Central Iowa Psychological Services

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Central Iowa Psychological Services:

By: _____

Print Name: Warren Phillips

Print Title: President

Date: 4/1/22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Cerro Gordo County

Chart of Account	Service Description	Unit of Service	Rate
75XXX	Mental Health Advocate	Monthly	See Other Terms

OTHER TERMS:
CICS will reimburse for Cerro Gordo County Mental Health Advocate expenses. Mental Health Advocate services are provided and funded for Cerro Gordo County. At the time of monthly billing, Mental Health Advocate will submit names of individuals served for the month of service.

Central Iowa Community Services:

By: _____

Print Name: _____

Print Title: Chair, CICS Governing Board

Date: _____

Cerro Gordo County:

By: Chris Watts

Print Name: Chris Watts

Print Title: Board Chair

Date: 5-31-22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Choices Therapy Services, LLC

Chart of Account	Service Description	Unit of Service	Rate
46305 Jail 42305 Outpatient	Therapy Evaluation (90791)	Visit	$155.61
46305 Jail 42305 Outpatient	Therapy 90837 90834 90832	 60 Min. 45 Min. 30 Min.	 $114.17 $114.17 $59.43
46305 Jail 42305 Outpatient	Group Therapy (90853)	Hour	$69.43
42305	Family Therapy (90846)	Hour	$98.83
42305	Individual - Behavioral Health Intervention Services (BHIS)	15 Min.	$21.88
42305	Family – Behavioral Health Intervention Services (BHIS)	15 Min.	$21.43

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Funding for outpatient services must be pre-authorized by CICS. CICS will issue a Notice of Decision to the patient and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Patients are responsible to pay all copayment amounts directly to the provider. CICS funds may supplement patients with insurance any remaining amount due, up to the "allowed charge" on the insurance Explanation of Benefits (EOB) or the contracted CICS rate, whichever is less.

Combined funding for Individual and Family BHIS shall not exceed 192 units for a 6 month funding authorization period. Units will be prorated for shorter funding authorization periods.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Choices Therapy Services, LLC:

By: _____

Print Name: Brenda L. Ward Clark

Print Title: Agency Owner

Date: 05/31/2022

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Eyerly Ball Community Mental Health Services

Chart of Account	Service Description	Unit of Service	Rate
32329	Supported Community Living – MI Home Based Habilitation High Recovery Recovery Transitional Medium Need Intensive I Intensive II Intensive III	 UA; .25-2 Hours/Day UB; 2.25-4 Hours/Day UC; 4.25-8.75 Hours/Day UD; 9-12.75 Hours/Day U8; 13-16.75 Hours/Day U9; 17-24 Hours/Day	 $54.09 $116.72 $135.28 $218.38 $221.40 $388.73
25376	Justice Coordination/Jail Diversion – Warren and Madison Counties	Monthly	$7,495.00*
42305	Therapy Evaluation (90791)	Visit	$155.61
42306	Psychiatric Evaluation (90792)	Visit	Dr $300.67 ARNP $232.09 PA $232.09
42305	Therapy 90837 90834 90832	 60 Min. 45 Min. 30 Min.	 $114.17 $114.17 $59.43
42306	Care Coordination	One Tele Health Session	$31.21
42305	Group Therapy (90853)	Hour	$69.43
42305	Family Therapy (90846)	Hour	$98.83
41305	Injection (96372)	N/A	$26.38
41305	Nursing (S9123)	Nurse Visit	$58.64
43301	Assessment, Evaluation, & Early Identification	Hour	$190.89
44301	Crisis Psychiatric Evaluation (2 appointments/month – Boone & Story)	Visit	Dr $300.67 ARNP $232.09 PA $232.09
44305	Community Based Crisis Intervention Services	Hour	$126.00
05373	Public Education, Prevention and Education Services	Hour	$126.00; Maximum of 12 hours/contract period
42306	Medication Management (99213)	15 Min.	Dr. $101.60 ARNP $72.45 PA $72.45
44307	Mobile Crisis Response (MCR) Service	Monthly	$93.474.72
44312	Crisis Stabilization Community Based Service (CSCBS)	Monthly	$17,804.71
44307	Mobile Crisis Response (MCR) Service	Monthly	$6,940.83

44312	Crisis Stabilization Community Based Service (CSCBS)	Monthly	$1,322.06
42398	Assertive Community Treatment (ACT)	Daily (Maximum of 5 Days/Week)	$55.83
42398	ACT Services Access Fee	Monthly Per Client	$290.00**
42396	Community Support Services (CSS) – Low Intensity	Monthly	$176.87
42396	Community Support Services (CSS) – High Intensity	Monthly	$520.02
42305	Licensed Independent Social Worker (LISW) Onboarding & Access for Laura Probasco July 1, 2022 – June 30, 2023	N/A	Maximum of $10,000.00***

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Provider will meet monthly with CICS, and if requested any other region covered under the contract if they request to meet monthly, to review MCR and CSCBS service provision, outcomes, and financials.

Provider will meet monthly with CICS to review Justice Coordination/Jail Diversion service provision, outcomes, and financials.

If structural or service provision changes take place for MCR, rates can be re-established.

Reconciliation of block grant funded services including MCR, CSCBS, and Justice Coordination/Jail Diversion may occur upon mutual agreement by the Provider and CICS, and any other region covered under the contract.

MCR Provider Outcomes:

- **MCR total response time regionwide and for each individual county shall be 60 minutes or less 85% of the time.**
- **No more than eight shifts per month for MCR will be phone response only.**
- **85% of the time on-call response staff will provide information to service recipients regarding local resources.**
- **Provide weekly contact information to CICS service coordination and have at least monthly interaction with local CICS service coordinators regarding resources and coordination of services.**

Psychological Testing is a service under Assessment, Evaluation, & Early Identification.

CICS may be billed the Crisis Psychiatric Evaluation rate if the Crisis Psychiatric Evaluation appointment is reserved and unfilled. Two Crisis Psychiatric Evaluation appointments shall be available monthly (every other week) for Boone and Story County. If crisis medication management is needed, this can be performed during the reserved crisis psychiatric evaluation time slot and billable at the contracted medication management reimbursement rate as applicable.

Public Education, Prevention and Education Services - Education services means activities that increase awareness and understanding of the causes and nature of conditions or factors which affect an individual's development and functioning. Prevention means efforts to increase awareness and understanding of the causes and nature of conditions or situations which affect an individual's functioning in society. Prevention activities are designed to convey information about the cause of conditions, situations, or problems that interfere with an individual's functioning or ways in which that knowledge can be used to prevent their occurrence or reduce their effect, and may include but are not limited to, training events, webinars, presentations, and public meetings. Provider outreach activities and/or marketing activities would not fall under Public Education, Prevention and Education. Provider needs to seek prior written approval by CICS for funding of Public Education, Prevention and Education services.

All funding for outpatient services must be pre-authorized by CICS. CICS will issue a Notice of Decision to the patient and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Patients are responsible to pay all copayment amounts directly to the provider. CICS funds may supplement patients with insurance any remaining amount due, up to the "allowed charge" on the insurance Explanation of Benefits (EOB) or the contracted CICS rate, whichever is less.

Established Polk County rates will be honored for outpatient services provided for Warren County.

Based on the client's individualized assessment, CICS will honor the Provider's Medicaid tiered rate for Supported Community Living Home Based Habilitation service. Documentation of the client's individualized assessment and the Medicaid tiered rate shall be provided to CICS by the Provider. If a current individualized client assessment is not available CICS will complete an assessment and work with the provider in identifying the applicable Medicaid tiered rate for the Individual. Individual rates may be reviewed at the request of CICS, or the Provider as determined necessary.

* For billing of Justice Coordination/Jail Diversion position must provide service for the entire month or rate is to be prorated. Monthly amount to be billed and reimbursed not to exceed $7,495.00/month for Warren and Madison County. At time of monthly billing submission for Justice Involved/Jail Diversion services, provider will submit documentation of participant names with hours served for month billed.

**ACT Services Access fee is to be prorated if ACT services are not provided for the entire month.

For MCR services provided within the CICS Region, up to $93,474.72 is the monthly amount to be billed/reimbursed when fully staffed based on budget provided. If employee positions are unfilled at any time, Provider needs to notify CICS to determine a monthly reimbursement up to the $93,474.72 based on the budget provided for this Agreement.

For MCR services provided within the Care Connections of Northern Iowa Region, up to $6,940.83 is the monthly amount to be billed/reimbursed when fully staffed based on budget provided. If employee

positions are unfilled at any time, Provider needs to notify CICS and Care Connections of Northern Iowa to determine a monthly reimbursement up to the $6,940.83 based on the budget provided for this Agreement.

For CSCBS provided within the CICS Region, up to $17,804.71 is the monthly amount to be billed/reimbursed when fully staffed based on budget provided. If employee positions are unfilled at any time, Provider needs to notify CICS to determine a monthly reimbursement up to the $17,804.71 based on the budget provided for this Agreement.

For CSCBS provided within the Care Connections of Northern Iowa Region, up to $1,322.06 is the monthly amount to be billed/reimbursed when fully staffed based on budget provided. If employee positions are unfilled at any time, Provider needs to notify CICS and Care Connections of Northern Iowa to determine a monthly reimbursement up to the $1,322.06 based on the budget provided for this Agreement.

MCR and CSCBS shall be billed by the 15th of each month. The Provider shall bill CICS and Care Connections of Northern Iowa the contracted monthly reimbursement amount for the prior month of MCR and CSCBS provided minus any MCR and CSCBS reimbursement received by Medicaid or other funders. At time of monthly billing submission, provider will submit documentation as agreed upon by Provider and CICS.

*****LISW will provide Outpatient Therapy Services to residents of CICS region and accept and provide services to patients with Medicaid and/or Medicare, private insurance, and MHDS regional funding. If the LISW is less than full-time and/or practices less than full-time in the Outpatient setting, the Access fee will be prorated based on the total number of hours LISW services are available to patients in the Outpatient setting.**

The LISW Onboarding & Access Fee shall be prorated if applicable and paid in the month of June 2023 for Fiscal Year 2023 with an invoice submitted by the provider.

In the event the LISW does not maintain employment with Eyerly Ball CMHC and upon initiation continue to provide Outpatient Therapy Services in the Outpatient setting for the entire CICS Provider and Program Participation Agreement service period ending June 30, 2023, no LISW Onboarding & Access Fee will be paid by CICS.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Eyerly Ball Community Mental HealthServices:

By: Cy Steidl Bishop

Print Name: Cynthia Steidl Bishop

Print Title: CEO

Date: 5/24/2022

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Hamilton County

Chart of Account	Service Description	Unit of Service	Rate
75XXX	Mental Health Advocate	Monthly	See Other Terms

OTHER TERMS:
CICS will reimburse for Hamilton County Mental Health Advocate expenses. Mental Health Advocate services are provided and funded for Hamilton County. At the time of monthly billing, Mental Health Advocate will submit names of individuals served for the month of service.

Central Iowa Community Services:

By: _____

Print Name: _____

Print Title: Chair, CICS Governing Board

Date: _____

Hamilton County:

By: Rick Young

Print Name: Rick Young

Print Title: Chairman, Bd of Supervisors

Date: 6-14-22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Hardin County

Chart of Account	Service Description	Unit of Service	Rate
75XXX	Mental Health Advocate	Monthly	See Other Terms

OTHER TERMS:
CICS will reimburse for Hardin County Mental Health Advocate expenses. Mental Health Advocate services are provided and funded per the established 28E Agreement with Hardin, Franklin, Marshall and Story Counties. At the time of monthly billing, Mental Health Advocate will submit names of individuals served for the month of service.

Central Iowa Community Services:

By: _____

Print Name: _____

Print Title: Chair, CICS Governing Board

Date: _____

Hardin County:

By: _____

Print Name: BJ Hoffman

Print Title: Chair

Date: 6/1/22

This Memorandum of Understanding (hereinafter "MOU") is entered into between Jasper County, Iowa and Central Iowa Community Services (CICS) Mental Health and Disability Services (MHDS) Region.

I. **Funding of Mental Health Advocate Services.** In recognition that Jasper County has entered into an agreement with Polk County and Marion Counties to share the expense of Judicial Advocate Services and that Judicial Advocate services are funded by MHDS Regions. This MOU establishes an agreement between Jasper County and CICS for the funding of Judicial Advocate services. In consideration, the following responsibilities are assumed by the participating agencies:

a. **Jasper County Responsibilities.** Jasper County agrees to:
   i. Ensure the delivery of Judicial Advocate services for residents of Jasper County in accordance with Section 229.19 of the Iowa Code.
   ii. Submit claim to CICS Claims for reimbursement of Judicial Advocate services based on Jasper County's share of the Judicial Advocate expenses. Submit claims for reimbursement per the CICS Management Plan Policies and Procedures: J. Service Provider Payment Provisions.

b. **CICS Responsibilities.** CICS agrees to:
   i. Fund Judicial Advocate services up to Jasper County's share of the Judicial Advocate expenses. Payment for service shall follow the CICS Management Plan Policies and Procedures: J. Service Provider Payment Provisions.

II. **Termination.** This MOU will be renewed on a fiscal year annual basis unless terminated earlier in writing by any party for its convenience upon sixty (60) days prior written notice to the other party. The agreement is subject to revision due to legislation, change in operating practices and policies of the involved parties, or other factors, as agreed to by the involved parties. It may be amended by mutual written agreement of the parties.

III. **Indemnification.** Jasper County shall defend, hold harmless and indemnify CICS against any and all claims, liability, damages, judgments, and expenses, including, without limitation, reasonable attorney fees and costs, asserted against, imposed or incurred by CICS that arise out of acts or omission of Advocate or County's employees, agents or representatives in the discharge of its responsibilities under this Agreement.

IV. **Notices.** All notices related to this MOU shall be addressed as follows:

a. To: CICS Operations Officer
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010

b. Jasper County Board of Supervisors:
Attn: Board Chair
Jasper County Courthouse
101 1st Street N, Newton, IA 50208

IN WITNESS WHEREOF, the parties have here unto set their hand, and the effective date of this agreement is the First day of July 2022.

CICS Governing Board:

By: _____

Print Name: _____

Print Title: Chair, CICS Governing Board

Date: _____

Jasper County Board of Supervisors:

By: Brandon Talsma

Print Name: Brandon Talsma

Print Title: Chair, Board of Supervisors

Date: 31 May 2022

Attest:

By: Dennis Parrott

Print Name: Dennis K. Parrott

Print Title: Auditor

Date: May 31, 2022

AGREEMENT FOR REIMBURSEMENT OF JUDICIAL HOSPITALIZATION REFEREE

This Agreement is between the State of Iowa Judicial Branch ("Judicial Branch") and Central Iowa Community Services, Iowa, ("CICS") as created under Iowa Code section 331.389 and approved by their board. The purpose of this agreement is to efficiently provide and pay for the services of a hospitalization referee who will conduct hospitalization proceedings in and around Cerro Gordo County. In order to achieve this purpose, the Judicial Branch and CICS agree to the following:

1. CICS and the Judicial Branch agree that safe, timely, and fair adjudication of hospitalization cases involving individuals who may be suffering from a serious mental impairment including multi-occurring disorders benefits all the parties who are involved in these proceedings.

2. In order to ensure that there are sufficient personnel available to handle the timely adjudication of hospitalization cases in and around Cerro Gordo County, the Judicial Branch will appoint a judicial hospitalization referee pursuant to Iowa Code section 229.21 to handle the cases in this area.

3. In exchange for CICS and the counties they represent receiving the benefit of the services of this judicial hospitalization referee, CICS agrees to reimburse the Judicial Branch an agreed upon monthly amount of money to financially support the local services of this referee.

4. The amount of financial support provided by CICS to the Judicial Branch will be $3,333.33 per month. The total amount of reimbursement for the services covered by this Agreement shall not exceed $40,000.00 per year.

5. Each month a statement of services provided by this hospitalization referee to the CICS member counties shall be submitted by the Judicial Branch to CICS. CICS and the Judicial Branch shall develop a format and process for the presentation of this statement that is mutually agreeable to both. Within 30 days of receiving the statement of services from the Judicial Branch, CICS shall reimburse the Judicial Branch for the full amount due.

6. In the event that the Iowa Legislature or other State Government takes action that results in the dissolution of Central Iowa Community Services (CICS) or the inability for CICS to pay for this service, this agreement will terminate at that time.

7. No new legal or administrative entity is created by this agreement. No joint or cooperative budget is created, nor are any new financial mechanisms being created. Nothing in this agreement shall affect any change with respect to ownership of the real or personal property of either party to this agreement, and any property acquired during the term of this agreement shall remain the property of the acquiring party.

8. The hospitalization referee who will be appointed pursuant to this agreement will not be an employee of CICS or any county. The right to hire, manage, discipline, and terminate the referee who will be appointed to this position rests solely with the Judicial Branch.

9. This agreement constitutes the entire agreement between the Iowa Judicial Branch and CICS regarding reimbursement for services of the judicial hospitalization referee, and it will be in full force and effect upon completion of the signing.

10. This agreement shall take effect July 1, 2022 and remain in effect until June 30, 2023 unless it is terminated prior to that time pursuant to the terms established in paragraph 11.

11. Either party may terminate this Agreement by providing at least sixty days written notice to the other party's representative, noted below. This written notice shall be sent by certified mail, return receipt requested. Termination of this agreement does not require a showing of cause.

Send Judicial Branch notice to:

State Court Administrator
Attn: Robert Gast
Iowa Judicial Branch
1111 E. Court Avenue
Des Moines, Iowa 50319

Send CICS notice to:

Central Iowa Community Services
Attn: Karla Webb
126 S. Kellogg Ave., Ste. 001
Ames, IA 50010

12. If any provision of this agreement is determined by a court of competent jurisdiction to be invalid or unenforceable, that shall not affect the validity or enforceability of any other provision of this agreement.

The undersigned hereby execute and enter into this agreement. Each of us represents that we have the authority in accordance with state law to sign and bind the entity we are representing.

FOR CENTRAL IOWA COMMUNITY SERVICES:

BJ Hoffman Date
Central Iowa Community Services

FOR THE IOWA JUDICIAL BRANCH:

6-3-22
Robert Gast Date
State Court Administrator

5/3/22
James M. Drew, Chief Judge Date
Second Judicial District

5-2-2022
Scott Hand, District Court Administrator Date
Second Judicial District

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Liberty Square dba Spring Harbor Residential Services

Chart of Account	Service Description	Unit of Service	Rate
32329	Supported Community Living – ID/DD	15 Min.	$9.28
32329	Supported Community Living – ID/DD without day service*	Tier 1 (U1); Daily Tier 2 (U2); Daily Tier 3 (U3); Daily Tier 4 (U4); Daily Tier 5 (U5); Daily Tier 6 (U6); Daily	$196.91 $211.09 $280.88 $284.00 $484.65 $648.61
32329	Supported Community Living – ID/DD with day service**	Tier 1 (U1); Daily Tier 2 (U2); Daily Tier 3 (U3); Daily Tier 4 (U4); Daily Tier 5 (U5); Daily Tier 6 (U6); Daily	$175.58 $189.17 $226.13 $229.26 $402.53 $555.55
32329	Supported Community Living - Home Based Habilitation High Recovery Recovery Transitional Medium Need Intensive I Intensive II Intensive III	 UA; .25-2 Hours/Day UB; 2.25-4 Hours/Day UC; 4.25-8.75 Hours/Day UD; 9-12.75 Hours/Day U8; 13-16.75 Hours/Day U9; 17-24 Hours/Day	 $54.09 $116.72 $135.28 $218.38 $221.40 $388.73

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Funding for all contracted services requires prior authorization and individuals shall meet CICS Management Plan criteria. CICS will issue a Notice of Decision to the client and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Clients are responsible to pay all copayment amounts directly to the provider.

Based on the client's individualized assessment, CICS will honor the Provider's Medicaid tiered rate for daily Supported Community Living service and Home Based Habilitation service. Documentation of the client's individualized assessment and the Medicaid tiered rate shall be provided to CICS by the Provider. If a current individualized client assessment is not available CICS will complete an assessment and work with the provider

in identifying the applicable Medicaid tiered rate for the Individual. Individual rates may be reviewed at the request of CICS or the Provider as determined necessary.

***Supported Community Living for individuals with an authorized average of 39 or fewer hours of service outside the home per month.**

****Supported Community Living for individuals with an authorized average of 40 or more hours of service outside the home per month.**

A billable unit for Supported Community Living services is defined as face-to-face contact with client. These units shall be rounded to the nearest quarter hour with a minimum of a quarter hour to be billed for each contact.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Liberty Square dba Spring Harbor Residential Services:

By: Kathy Fanchon

Print Name: Kathy Fanchon

Print Title: Exc Director

Date: 9/1/22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Mason City Clinic

Chart of Account	Service Description	Unit of Service	Rate
42306	Psychiatric Evaluation (90792)	Visit	Dr. $300.67 ARNP $232.09 PA $232.09
42306	Medication Management (99213)	15 Min.	Dr. $101.60 ARNP $72.45 PA $72.45
74300	Commitment Testimony – Doctor testimony in person or by phone	Per Testimony	$60.00

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Funding for outpatient services must be pre-authorized by CICS. CICS will issue a Notice of Decision to the patient and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Patients are responsible to pay all copayment amounts directly to the provider. CICS funds may supplement patients with insurance any remaining amount due, up to the "allowed charge" on the insurance Explanation of Benefits (EOB) or the contracted CICS rate, whichever is less.

For payment of Commitment Testimony services a completed funding application must be received.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Mason City Clinic:

By: Mark Mulky

Print Name: Mark Mulky

Print Title: President

Date: 6/6/22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Orchard Place

Chart of Account	Service Description	Unit of Service	Rate
05373	Public Education, Prevention and Education	Hour	$126.00; Maximum of 12 hours/contract period
42305	Individual - Behavioral Health Intervention Services (BHIS)	15 Min.	$21.88
42305	Family – Behavioral Health Intervention Services (BHIS)	15 Min.	$21.43

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

CICS Region will honor rates established by the provider's host region for outpatient services.

Public Education, Prevention and Education Services - Education services means activities that increase awareness and understanding of the causes and nature of conditions or factors which affect an individual's development and functioning. Prevention means efforts to increase awareness and understanding of the causes and nature of conditions or situations which affect an individual's functioning in society. Prevention activities are designed to convey information about the cause of conditions, situations, or problems that interfere with an individual's functioning or ways in which that knowledge can be used to prevent their occurrence or reduce their effect, and may include but are not limited to, training events, webinars, presentations, and public meetings. Provider outreach activities and/or marketing activities would not fall under Public Education, Prevention and Education. Provider needs to seek written approval by CICS for funding of Public Education, Prevention and Education services.

Funding for outpatient services must be pre-authorized by CICS. CICS will issue a Notice of Decision to the patient and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Patients are responsible to pay all copayment amounts directly to the provider. CICS funds may supplement patients with insurance any

remaining amount due, up to the "allowed charge" on the insurance Explanation of Benefits (EOB) or the contracted CICS rate, whichever is less.

Combined funding for Individual and Family BHIS shall not exceed 192 units for a 6 month funding authorization period. Units will be prorated for shorter funding authorization periods.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Orchard Place:

By: Valerie Sattsgaver

Print Name: Valerie Sattsgaver

Print Title: CFO

Date: 5/31/22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Pillar of Cedar Valley

Chart of Account	Service Description	Unit of Service	Rate
64317	Nursing Facility ICF/PMI	Daily	$278.27

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Funding for all contracted services requires prior authorization and individuals shall meet Pre-Admission Screening and Resident Review (PASRR) level of care and CICS Management Plan criteria. CICS will issue a Notice of Decision to the client and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Clients are responsible to pay all copayment amounts directly to the provider.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Pillar of Cedar Valley:

By: _____

Print Name: Hilary Schmidt

Print Title: _____

Date: 5/26/22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Region 6 Resource Partners

Chart of Account	Service Description	Unit of Service	Rate
31354	Grinnell Demand Response	One way ride	$3.00
31354	Iowa Falls Demand Response	One way ride	$3.00
31354	Tama/Toledo Demand Response	One way ride	$3.00
31354	South Tama County to Marshalltown on Routes	Per Mile	$2.79
31354	Hardin, Marshall, Poweshiek, Tama County Deal Days	One way ride	$7.00
31354	Marshalltown Demand Response (Some medical facilities may reduce the ride cost to their destination)	One way ride	$7.00
31354	Rides originating and ending at other places. Shall use www.mapquest.com to determine mileage from residence to destination. Only miles where passenger is on board shall be used for this calculation.	Per mile	$2.79

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

Funding for all contracted services requires prior authorization and individuals shall meet CICS Management Plan criteria. CICS will issue a Notice of Decision to the client and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Clients are responsible to pay all copayment amounts directly to the provider.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Region 6 Resource Partners:

By: _____

Print Name: Marty Wymore

Print Title: Director

Date: 6/13/22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Rodasi LLC, dba Midwest Counseling

Chart of Account	Service Description	Unit of Service	Rate
42305	Therapy Evaluation (90791)	Visit	$155.61
42306	Psychiatric Evaluation (90792)	Visit	Dr. $300.67 ARNP $232.09 PA $232.09
42305	Therapy 90837 90834 90832	 60 Min. 45 Min. 30 Min.	 $114.17 $114.17 $59.43
42306	Medication Management (99213)	15 Min.	Dr. $101.60 ARNP $72.45 PA $72.45
42305	Group Therapy (90853)	Hour	$69.43
42305	Family Therapy (90846)	Hour	$98.83

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

All funding for outpatient services must be pre-authorized by CICS. CICS will issue a Notice of Decision to the patient and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Patients are responsible to pay all copayment amounts directly to the provider. CICS funds may supplement patients with insurance any remaining amount due, up to the "allowed charge" on the insurance Explanation of Benefits (EOB) or the contracted CICS rate, whichever is less.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Rodasi LLC, dba Midwest Counseling:

By: Stephen Boyns

Print Name: Stephen Boyns

Print Title: CEO

Date: 6-3-22

ATTACHMENT A
SERVICE DEFINITIONS AND RATES
Youth Shelter Care of North Central Iowa, Inc.

Chart of Account	Service Description	Unit of Service	Rate
42306	Psychiatric Evaluation (90792)	Visit	Dr. $300.67 ARNP $232.09 PA $232.09
42306	Medication Management (99213)	15 Min.	Dr. $101.60 ARNP $72.45 PA $72.45
42305	Therapy Evaluation (90791)	Visit	$155.61
42305	Therapy 90837 90834 90832	 60 Min. 45 Min. 30 Min.	 $114.17 $114.17 $59.43
42305	Group Therapy (90853)	Hour	$69.43
42305	Family Therapy (90846)	Hour	$98.83
42305	Individual - Behavioral Health Intervention Services (BHIS)	15 Min.	$21.88
42305	Family – Behavioral Health Intervention Services (BHIS)	15 Min.	$21.43
44313	Crisis Stabilization Residential Services (CSRS)	Daily	$360.19
44313	CSRS Family Team Decision Making (FTDM) Services	One Time Per CSRS Admission	$400.00

OTHER TERMS:

Medicaid/MCO floor rate may be honored if higher than the CICS Contracted Rate. Please send documentation of the Medicaid/MCO rate to the Operations Officer for consideration of the rate adjustment. If the rate adjustment is approved by CICS this will be executed through a written document with the CICS CEO and the Provider with the effective date as the month following the receipt of the rate documentation. A CICS contract amendment will not be required in these situations.

All funding for outpatient services must be pre-authorized by CICS. CICS will issue a Notice of Decision to the patient and provider. CICS will determine the copayment for persons as specified in the CICS Management Plan. Patients are responsible to pay all copayment amounts directly to the provider. CICS funds may supplement patients with insurance any remaining amount due, up to the "allowed charge" on the insurance Explanation of Benefits (EOB) or the contracted CICS rate, whichever is less.

Combined funding for Individual and Family BHIS shall not exceed 192 units for a 6 month funding authorization period. Units will be prorated for shorter funding authorization periods.

CSRS – MHDS Regional funding pertains to non-system involved youth. Provider will seek Medicaid or Private Insurance funding when applicable. Upon exhaustion of Medicaid/Private Insurance if additional funding is needed, Provider may notify designated CICS Regional staff to request CICS funding not to exceed a total of 14 days from day of CSRS admit.

When no other funding is applicable, provider will notify designated CICS Regional staff within 24 hours of CSRS admission or next business day if admission occurs on weekend or holiday. Region will fund a maximum of 14 days. Provider will submit required paperwork to Regional staff for the funding authorization process.

CSRS FTDM fee – this applies to youth funded for CSRS services by MHDS Regions.

Central Iowa Community Services:

By: _____

Print Name: BJ Hoffman

Print Title: Chair, CICS Governing Board

Date: _____

Youth Shelter Care of North Central Iowa, Inc.:

By: Patricia A Cirks

Print Name: Patricia S. Cirks

Print Title: Executive Director

Date: 5/27/22