Heritage Area Agency on Aging

POLICIES AND PROCEDURES

RELATING TO THE

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, HITECH AND THE HIPAA PRIVACY, SECURITY, ENFORCEMENT AND BREACH NOTIFICATION OMNIBUS FINAL RULE

HIPAA

TABLE OF CONTENTS

HERITAGE AREA AGENCY ON AGING
HYBRID ENTITY DESIGNATION

Heritage Area Agency on Aging, in effort to comply with the provisions of the Administrative Simplification Regulations of the Health Insurance Portability and accountability Act ("HIPAA"), 45 C.F.R. § 164.105(c)(1), makes the following designation of activities:

HIPAA Covered Activities	Activities Not Subject to HIPAA[1]
Adult Day Health Services	Nutrition Programming
Case Management	Volunteer Transportation Programming
Elder Abuse Prevention and Awareness	Legal Services
Respite	Training and Education Programming
Options Counseling	Information & Assistance
	Caregiver Programming
	Outreach
	Advocacy
	Material Aid
	Older Worker Program
	Chore
	Evidence-Based Programming

Heritage included in its covered health care components those programs that would meet the definition of "covered entity" if each were a separate legal entity. This means that only the programs identified under "HIPAA Covered Activities," above, are required to comply with the Privacy and Security Rules under HIPAA. Nonetheless, Heritage has implemented confidentiality and security policies agency-wide that incorporate many of the HIPAA standards. This list could change in the future and thus Heritage will update this Hybrid Entity disclosure on a biannual basis.

Determining that Heritage is a hybrid entity means that the release of PHI from a covered component to a non-covered component is considered a disclosure under HIPAA and is not permitted unless there is an individual authorization or a specific exemption allowing the disclosure. The Privacy Rule requires Heritage to implement protections between the covered and non-covered components to assure that PHI is not improperly disclosed.

For subcontracted services that are associated with HIPAA Covered Activities, a Business Associate Agreement is maintained. Non-covered activities are not required to enter into Business Associate Agreements.

[1] Several of Heritage's programs that contract for the provision of health care are not required to be included in the covered component because they do not transmit health information in electronic form in connection with one of the standard transactions specific in the regulations. See 45 C.F.R. § 160.103 (definition of transaction).

Policy 1
Transition provisions

Policy:

Heritage Area Agency on Aging will comply with federal privacy regulations for Protected Health Information during the transition period surrounding July 1, 2006.

Procedure:

1. Use or disclosure of Protected Health Information: For PHI created or received prior to July 1, 2006, Heritage Area Agency on Aging may use or disclose that PHI after July 1, 2006, provided
   - An authorization or release of information was obtained, or
   - The authorization or release of information does not contain any agreed to restrictions. (*See policy for Right of an individual to request restriction of uses and disclosures)

2. Effect of prior contracts or other arrangements with Business Associates: Heritage Area Agency on Aging may disclose PHI to a Business Associate and may allow a Business Associate to create, receive or use PHI on its behalf as long as there is a written contract or other written arrangement in place with the Business Associate and the agreement or contract was entered into prior to July 1, 2006. This contract satisfies the Business Associate requirement.

Policy 2
Notice of Privacy Practice For
Protected Health Information

Policy:

Heritage Area Agency on Aging shall provide written notice to the client or responsible party about how the agency may use or disclose the client's protected health information. This includes the individual's rights and the agency's legal duties with respect to protected health information.

Procedure:

1. Heritage Care Program Team Members will be supplied with copies of the Acknowledgement of Receipt of the Notices of Privacy Practices and the accompanying signature form.

2. All individuals will receive a copy of the agency's notice of privacy practice at the first face-to-face contact for services provided DIRECTLY by the agency. In an emergency treatment situation, the notice of privacy practice will be made available as soon as reasonably practical afterwards.

3. Each individual will be asked to sign a written acknowledgement that the notice has been made available. If the individual refuses, after a good faith attempt of staff to obtain the acknowledgement, staff will document the reason why the acknowledgement was not obtained.

4. At direct service delivery sites, the privacy practice notice will be available for individuals to take with them and the Notice of Privacy Practice will also be posted in a clear and prominent position.

5. The Notice of Privacy Practice may be provided to an individual by email if the individual agrees to electronic notice. A recipient of electronic notice retains the right to obtain a paper copy of the notice upon request. If any services are provided electronically, a privacy notice must be made available to the individual at the first face-to-face visit for direct service.

6. The Notice of Privacy Practice will be posted in a prominent section of the web site and a notice will be available electronically through the web site. Notice of updated versions of the Notice of Privacy Practice will be posted on the website.

7. All agency staff members will be responsible for making the privacy notice available to all clients receiving DIRECT service with written acknowledgement documented in the client record of service.

8. Audits of clinical records will demonstrate compliance with procedure.

9. All copies of notices of privacy practices will be retained for 6 years or according to the agency record retention polices.

Notice of Privacy Practices

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.

Heritage Area Agency on Aging is required by law to maintain the privacy of your health information and to provide you with notice of its legal duties and privacy practices with respect to your health information. If you have any questions about this Notice, please contact our Privacy Officer at 319-398-5559 or 1-800-332-5934.

USE AND DISCLOSURE OF HEALTH INFORMATION

Heritage collects health information from you and stores it in a record or on a computer. This record is the property of Heritage, but the information in the record belongs to you. Heritage may use your health information for purposes of providing you treatment, obtaining payment for your care and conducting health care operations. Heritage has established policies to guard against unnecessary disclosure of your health information. Heritage may use or disclose your health information for the following purposes:

Treatment. Heritage may use your health information to coordinate care within Heritage and with others involved in your care such as your attending physician, service providers, and other health care professionals who have agreed to assist Heritage in coordinating care. Heritage may also disclose your health information to individuals outside of Heritage involved in your care including family members, clergy who you have designated, pharmacists, suppliers of medical equipment, dieticians or other health care professionals.

Conduct Health Care Operations. Heritage may use and disclose health information for its own operations in order to facilitate the function of Heritage and as necessary to provide quality services to all of Heritage's clients. Health care operations include such activities as evaluating the quality of health care services, compliance with federal and state regulations, case management and care coordination, professional review and performance evaluation, business planning and development and general administrative activities of Heritage. For example, Heritage may use your health information to evaluate its staff performance, combine your health information with other Heritage clients in evaluating how to more effectively serve all of its clients, disclose your health information to Heritage staff and contracted personnel for training purposes, use your health information to contact you as a reminder regarding a visit to you, or contact you as part of general fundraising and community information mailings unless you tell us you do not want to be contacted.

Obtain Payment. Heritage may include your health information on invoices to collect payment from third parties for the care you receive from Heritage. For example, Heritage may be required by the federal or state government to provide information regarding your health care status so that the federal or state government will reimburse you or Heritage. Heritage may also need to obtain prior approval from your insurer or state or federal government and may need to explain your need for services that would be provided to you.

Fundraising Activities. Heritage may use information about you including your name, address, phone number, and the dates you received services in order to contact you or your family to raise money for

Heritage. If you do not want Heritage to contact you or your family, notify the Privacy Officer and indicate that you do not wish to be contacted.

OTHER USE AND DISCLOSURE OF HEALTH INFORMATION

Legally Required. Heritage will disclose your health information when it is required to do so by any federal, state or local law.

Risks To Public Health. Heritage may disclose your health information for public activities and purposes in order to prevent or control disease, injury, disability, report abuse or neglect, report domestic violence, report to the Food and Drug Administration problems with products and reactions to medications and to report disease or infection exposure.

Health Oversight Activities. Heritage may disclose your health information to a health oversight agency for activities including audits, civil administrative or criminal investigations, inspections, licensure or disciplinary action. Heritage may not disclose your health information if you are the subject of the investigation and your health information is not directly related to your receipt of healthcare or public benefits.

Judicial and Administrative Proceedings. Heritage may disclose your health information in the course of any judicial or administrative proceeding in response to an order of a court or administrative tribunal as expressly authorized by such order or in response to a subpoena, discovery request or other lawful process but only when Heritage makes reasonable efforts to either notify you about the request or to obtain an order protecting your health information.

Law Enforcement Purposes. Heritage may disclose your health information to a law enforcement official for purposes, such as identifying or locating a suspect, fugitive, material witness or missing person, complying with a court order or subpoena or other law enforcement purpose.

Deceased Person Information. Heritage may disclose your health information to coroners, medical examiners and funeral directors.

Health and Safety. In the event of a serious health threat to health or safety, Heritage may, consistent with applicable law and ethical standards of conduct, disclose your health information if Heritage in good faith believes that such disclosure is necessary to prevent or lessen a serious and imminent threat to your health or safety or to the health and safety of the public.

Specialized Governmental Functions. Heritage may disclose your health information for military, national security, prisoner and government to benefit purposes.

Workers ' Compensation. Heritage may disclose your health information as necessary to comply with workers' compensation laws.

AUTHORIZATION TO USE OR DISCLOSE HEALTH INFORMATION.

For purposes not described above, including uses and disclosures of PHI for marketing purposes, disclosures that would constitute a sale of PHI and most sharing of psychotherapy notes, Heritage will ask for your authorization before using or disclosing PHI. If you authorize Heritage to use or disclose your health information, you may revoke that authorization in writing at any time. A revocation of authorization will be effective on the date it is received and will not affect previous disclosures.

BREACH NOTIFICATION.

Heritage is required to provide you with notification if it discovers a breach of your unsecured protected health information that may have compromised the privacy or security of your information. You will be

notified without unreasonable delay and no later than 60 days after discovery of the breach. Such notification will include information about what happened and what can be done to mitigate any harm.

YOUR RIGHTS WITH RESPECT TO YOUR HEALTH INFORMATION. You have the following rights regarding your health information that Heritage maintains:

Right To Request Restrictions. You may request restrictions on certain uses and disclosures of your health information. You have the right to request that Heritage limit disclosure of your health information to someone who is involved in your care or payment for your care. Heritage is not required to agree to this request. If you have paid for services out-of-pocket, in full, you may request that Heritage not disclose PHI related solely to those services to a health plan. Heritage must accommodate this request, except where Heritage is required by law to make a disclosure. If you wish to make a request for restriction, contact the Privacy Officer, Heritage Area Agency on Aging, 6301 Kirkwood Blvd. SW, Cedar Rapids, IA 52404.

Right To Inspect and Copy Your Health Information. You have the right to inspect and copy your health information. A request to inspect and copy records containing your health information may be made to the Privacy Officer identified below. If you request a copy of your health information, Heritage may charge a reasonable fee for copying.

Right To Receive Confidential Communications. You have the right to request that Heritage communicate with you in a certain way. For example, you may ask that Heritage only conduct communications pertaining to your health information with you privately with no other family members present. If you wish to receive only confidential communications, contact the Privacy Officer identified below. Heritage will not request that you provide any reason for your request and will attempt to honor your reasonable request for confidential communications.

Right To Amend Health Information. You or your representative has the right to request that Heritage amend your records if you believe that your health information is incorrect or incomplete. That request may be made as long as the information is maintained by Heritage. A request for amendment should be made in writing to the Privacy Officer identified below. Heritage may deny the request if it is not in writing or does not include a reason for the amendment. The request may also be denied if your health information records were not created by Heritage, if the records you are requesting are not part of Heritage's record, if the health information you wish to amend is not part of the health information you or your representative are permitted to inspect and copy or if, in the opinion of Heritage, the records containing your health information are accurate and complete.

Right to Accounting of Disclosures. You have a right to receive an accounting of disclosures of your health information made by Heritage in the six years prior to the date of your request. The request for an accounting must be made in writing to the Privacy Officer identified below. Heritage will provide the first accounting during any 12-month period without charge. Subsequent accounting requests may be subject to a reasonable cost-based fee.

Right to Copy of Notice. You have a right to a paper copy of this Notice of Privacy Practices.

DUTIES OF HERITAGE: Heritage is required to abide by the terms of this Notice as it may be amended from time to time. Heritage reserves the right to change the terms of this Notice and to make the new Notice provisions effective for all health information that it maintains. If Heritage changes this

Notice, Heritage will provide a copy of the revised Notice to you or your representative. You or your representative has the right to express complaints to Heritage or to the Secretary of the Department of Health and Human Services if you believe that your privacy rights have been violated.

For further information, please contact:

Privacy Officer
Heritage Area Agency on Aging
6301 Kirkwood Blvd. SW
Cedar Rapids, IA 52404
(319) 398-5559

Heritage encourages you to express any concerns that you may have regarding the privacy of your information. If you are not satisfied with the manner in which Heritage handles a complaint, you may submit a formal complaint to:

Department of Health and Human Services
Office of Civil Rights
Hubert H. Humphrey Building
200 Independence Avenue S.W. Room 509F
Washington, DC 20201.

You will not be retaliated against in any way for filing a complaint.

Effective Date. This Notice is effective September 23, 2013.

Acknowledgement of Receipt of the Notice of Privacy Practices

I understand, that under the Health Insurance Portability & Accountability Act of 1996 (HIPAA), I have certain rights to privacy regarding my protected health information (PHI). The Notice of Privacy Practices has been made available to me, which explains those rights.

_____

(Client's Signature) *(Date)*

Print Client's Name: _____

_____

(Legal Representative Signature if applicable) *(Date)*

Print Name: _____

Relationship of representative to client: _____

Policy 3
Uses or Disclosures to Carry Out Treatment, Payment, or Health Care Operations

Policy:

Heritage Area Agency on Aging will use or disclose protected health information (PHI) to carry out **treatment, payment, or health care operations.** A consent is not required if use or disclosure is for treatment, payment, or health care operations of Heritage Area Agency on Aging.

Procedure:

1. Upon admission or the first date of service after July 1, 2006, agency staff will continue to request individual consent for service, but the consent to use and disclose PHI will not be obtained when the PHI is used for treatment, payment and health care operations of Heritage Area Agency on Aging.

2. Consent will not be obtained for disclosure of PHI for treatment activities of a health care provider.

3. Consent will not be obtained for disclosure of PHI to another covered entity or health care provider for agency payment activities.

4. Consent will not be obtained for disclosure of PHI to another covered entity that needs the PHI for health care operations activities and both Heritage and the other covered entity have a relationship with the individual. These activities include:

    a. Conducting quality assessment and improvement activities including evaluation and development of clinical guidelines, provided that the obtaining of generalized knowledge is not the primary purpose of any studies resulting from the activity.

    b. 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 Clients with information about treatment alternatives.

    c. Related functions that do not include treatment.

    d. Health care fraud and abuse detection or compliance.

Policy 4
Uses and Disclosures for Which an Authorization is Required

Policy:

Heritage Area Agency on Aging will not use or disclose Protected Health Information (PHI) without a valid Authorization unless otherwise permitted for treatment, payment or health care operations. See Policy 3. When an authorization is obtained, the use or disclosure must comply with the specifics of the authorization.

Procedure:

1. On admission or first date of service on or after July 1, 2006, determine if an authorization is needed.
2. Review the purpose of the authorization with the individual.
3. Ask the individual to read, complete, sign, and date the authorization form.
4. Place the completed authorization form in the individual's record.
5. Explain the right of revocation.
6. A copy of the authorization will be provided to the individual.
7. Each individual will be required to sign an Authorization form before PHI can be used or disclosed for psychotherapy notes, Substance Abuse, HIV/Aids records and marketing.
8. The authorization form will not be combined with any other document. The only time authorization can be combined is:
    - When an authorization for use or disclosure of psychotherapy notes is combined with another authorization for use or disclose of psychotherapy notes.
9. If marketing communication is face-to-face or the individual receives a promotional gift of nominal value, authorization is not required.
10. An authorization is not required when Heritage Area Agency on Aging must defend itself in a legal action or another proceeding brought by the individual.
11. An individual will be not forced to sign an authorization as a condition of the usual provision of treatment.
12. An individual may, at any time, revoke an authorization. The revocation must be in writing and will become part of the individual's records.
13. Any use or disclosure of PHI done under a valid authorization and prior to the revocation cannot be considered for sanction against Heritage or its staff.
14. All authorizations will be retained in the individual's record according to the record retention policy of 6 years, or whichever is the longest.
15. A valid authorization will be written in plain language and will contain:
    - A clear and specific description of the information to be used or disclosed
    - The name of the person or class of persons authorized to make the requested use or disclosure
    - The name of the person or class of persons who will receive the request for use or disclosure

- A description of the purpose of the requested use or disclosure. The statement "at the request of the individual" is sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- An expiration date or an expiration event that relates to the individual or the purpose of the authorization.
- Signature of the individual and date. When signed by a personal representative, the description of the representative's authority is required.
- The individual's right to revoke the authorization, with exceptions to revocation.
- The inability to condition treatment or payment on signing an authorization when applicable
- The potential for information disclosed under the authorization to be subject to re-disclosure by the recipient.

16. In the absence of a required release for HIPAA-covered activities, Care Program Team Members shall use the release located at pp. 13-15 of this Policy.

AUTHORIZATION TO RELEASE AND/OR OBTAIN PROTECTED HEALTH INFORMATION

SECTION I.

Re**:** DOB:

I, the undersigned, authorize Heritage Area Agency on Aging to release or obtain information verbally or in writing concerning the individual named above with:

Name of individual or agency Phone Number

Address City/State Zip Code

The information released or obtained may include:

_____

_____

_____

This authorization will automatically expire one year from the date of signature or as specified. _____
(Specific number of days or month)

I understand I may revoke this consent before expiration by sending a written notice to Heritage Area Agency on Aging, 6301 Kirkwood Blvd SW, Cedar Rapids, IA 52404. I understand that the release of information before this authorization expires or is revoked is not a breach of my rights of confidentiality. I understand that information disclosed under this authorization might be redisclosed by the recipient (except as noted below in Section II for the release of HIV-related, alcohol or drug treatment or mental health treatment information) and this redisclosure may no longer be protected by federal or state law. I also understand that I may refuse to sign this release and that treatment, payment, enrollment or eligibility for benefits will not be contingent on my signing. In addition, I have received a copy of this form.

Signature (self) Date

Signature of legal representative(s) Relationship Date

Heritage Representative Date

SECTION II.

SPECIFIC AUTHORIZATION FOR RELEASE OF INFORMATION PROTECTED BY STATE OR FEDERAL LAW

I specifically authorize the release information relating to (check the appropriate box(es)):

☐ Mental Health (includes psychological testing) information from:*

_____

_____

_____

☐ Substance Abuse (alcohol/drug abuse) information from:

_____

_____

_____

☐ HIV-Related Information (AIDS-related testing) from:

_____

_____

_____

Furthermore, I specifically authorize disclosure of this confidential information to the following persons or class of persons:

_____

In order for the information to be released, you must sign here AND at the end of Section I.

This authorization is valid for information already in existence and any information that may be generated while this authorization is effective. I understand that I have the right to see any information that is disclosed pursuant to this authorization for release. I may request to see this information during normal business hours. I understand that I can revoke my authorization at any time. I understand that the revocation will not apply to information that has already been released in response to this authorization. Unless otherwise revoked, this authorization shall expire on the date specified below. I understand that authorizing the disclosure of this information is voluntary. I can refuse to sign this authorization. I need not sign this form in order to assure treatment. I have read this form, or it has been read and explained to me, and I understand its content.

_____

Signature (Self) Date

_____

Signature of legal representative Relationship Date

*Only a person 18 years of age or older or a person's legal representative can authorize release of mental health information.

Federal and/or State law specifically require that any disclosure or redisclosure of substance abuse, alcohol or drug, mental health, or AIDS-related information must be accompanied by the following written statements:

Notice to Recipients of Mental Health Information

In accordance with "Disclosure of Mental Health and Psychological Information" (Iowa Code, Chapter 228), a recipient of mental health information may further disclose this information only with the written authorization of the subject or the subject's legal representative or as otherwise provided in Chapters 228 and 229. Unauthorized disclosure is unlawful and civil damages and criminal penalties may apply. Federal confidentiality rules (42 CFR Part 2) restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

Notice to Recipients of Substance Abuse Information

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.

Notice to Recipients of HIV-Related Testing Information

This information has been disclosed to you from records whose confidentiality is protected by state law. State law prohibits you from making any further disclosure of the information without specific written consent of the person to whom it pertains, or as otherwise permitted by law. A general authorization for the release of medical or other information is not sufficient for this purpose. (Iowa Code 141A.9.) Federal confidentiality rules (42 CFR, Part 2) restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

Policy 5
Confidentiality

I PURPOSE

To ensure that personal health information is protected so that individuals are not afraid to seek health care or to disclose sensitive information to health professionals. To also ensure that personal health information is protected during its collection, use, disclosure, storage, and destruction within Heritage Area Agency on Aging.

II DEFINITIONS

A. "Personal Health Information" means all information, recorded or exchanged verbally about an identifiable individual that relates to:

1. The individual's health or health care history, including genetic information about the individual or the individual's family.

2. What Heritage has learned or observed, including conduct or behavior that may be a result of illness or the effect of treatment.

3. The provision of health care to the individual. Individuals include co-workers or families of co-workers when they are clients of Heritage.

4. Payment for healthcare provided to the individual, which includes:
    a. The personal health identification number and any other identifying number, symbol, etc., assigned to an individual.
    b. Any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care.

B. Persons associated with Heritage: includes all employees, contracted individuals, volunteers, and students.

III POLICY

A. All employees and persons associated with Heritage are responsible for protecting the privacy and security of personal health information (oral or recorded in any form) that is obtained, handled, learned, heard or viewed in the course of their work or association with Heritage.

B. Personal health information shall be protected during its collection, use, storage and destruction with Heritage.

C. Use or disclosure of personal health information is acceptable only in the discharge of one's responsibilities and duties (including reporting duties imposed by legislation) and based on the need to know. Discussion regarding personal health information should not take place in the presence of persons not entitled to such information or in public places (elevators, lobbies, cafeteria, off premises, etc.)

D. The execution of a Personal Health Information Pledge of Confidentiality (see attached) is required as a condition of employment/contract/association/appointment with Heritage. Heritage employees are to sign a confidentiality pledge on an annual basis.

E. Unauthorized use of disclosure of confidential or protected health information will result in disciplinary action up to and including termination of employment/contract association/appointment.

F. All individuals who become aware of a possible breach of the security or confidentiality of personal health information are to follow the procedures outlined in Section IV.

IV PROCEDURE FOR ALLEGED BREACH OF CONFIDENTALITY

A. An allegation of a breach of confidentiality of personal health information may be made about any staff member of Heritage. Any individual receiving an allegation of a breach of confidentiality or having knowledge of a reasonable belief that a breach of confidentiality of personal health information may have occurred should immediately notify the Privacy Officer.

B. The Privacy Officer will decide whether to proceed with an investigation. It may be decided that a complaint does not require investigation if:
    1. The length of time that has elapsed since the date of complaint makes an investigation no longer practicable or desirable.

    2. The subject matter of the complaint is trivial or not made in good faith or is frivolous.

    3. The circumstances of the complaint do not require investigation.

C. If the decision is made to proceed with an investigation, it is the responsibility of the Privacy Officer to investigate the allegation and consult appropriate resources to make a determination if a breach of confidentiality of personal health information has been made.

D. If a breach of confidentiality of personal health information has occurred, disciplinary action should be taken.

E. All incidents of a breach of confidentiality of personal health information should be documented and filed in the employee's file and the office of the Privacy Officer.

Pledge for Confidentiality
Protected Personal Health Information

I, the undersigned, have read and understand Heritage Area Agency on Aging's policy on "Confidentiality Protected Personal Health Information Policy" as well as Heritage Area Agency on Aging's Information Security Policy. In consideration of my employment or association with Heritage 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 or after my employment or association ends, access or use personal health information, or reveal or disclose to any persons within or outside Heritage, any personal health information except as may be required in the course of my duties and responsibilities and in accordance with applicable legislation and agency policies governing proper release of information. I also understand that unauthorized use or disclosure of such information will result in disciplinary action up to and including termination of employment/contract/association and may result in the imposition of fines pursuant to applicable state and federal laws.

_____

Date

_____

Signature of individual making pledge

I have discussed the Confidentiality Protected Personal Health Information Policy and the consequences of a breach with the above named individual.

_____

Signature of individual administering pledge

_____

Date

Policy 6
Right to Restrict Use of Protected Health Information and Right to Confidential Communication

Policy:

Heritage Area Agency on Aging will permit an individual the right to request restriction of uses and disclosures of PHI (Protected Health Information); however, there is no requirement that Heritage agree to the requested restriction. An agreed-to restriction will be honored except in an emergency if the restricted PHI is needed to provide emergency treatment. Further disclosure of restricted PHI is prohibited for any other covered entity involved in the emergency treatment. A restriction is not effective if the restricted information is requested by the Secretary of the Department of Health and Human Services for compliance issues or if release of information falls under use and disclosures for public health activities. (See uses and disclosures for which an authorization or opportunity to agree or object is not required)

Procedure:

Request for restriction of PHI

1. An individual must submit a written request to restrict use and disclosure to his or her Care Program Team Member. The request must include the specific restriction and to whom the restriction will apply.
2. The Care Program Team Member will assist any client requesting that PHI not be shared with specific entities or individuals to complete a request of Restrict Use and Disclosure of Protected Health Information form (p. 21) and inform the client that some requests may not be honored as outlined in the Heritage HIPAA Manual.
3. Care Program Team Members (and Subcontracting Team Members) will bring any such requests to the attention of the Privacy Officer for approval.
4. As promptly as possible, the Privacy Officer will determine whether the restriction will be honored. The Privacy Officer will provide a copy of any requests to the Heritage Privacy Officer.
5. If the restriction is honored, a copy will be placed in the client's record. All appropriate staff will be notified of any restrictions. The outside of the client record will be flagged "Restricted Uses and Disclosures Approved." A colored sticker will be applied to the outside of the record. Heritage Care Program Team Members (and Subcontracting Team Members) will also indicate this restriction in the Case Management Database.
6. Any documentation or communication regarding restriction will comply with agency documentation policies. Anyone accessing or copying a record or database must check to see if there is a restriction on uses and disclosures. If one is found, the restriction must be read thoroughly to determine if it applies to the use intended. Any employee who is unsure whether the restriction applies or how it should apply should consult the Privacy Officer or the Privacy Officer. All documentation must be maintained for a period of six years from the date of creation or the date when it was last in effect, whichever is later.
7. If a request for disclosure comes from an outside entity asking for information that is restricted, the staff person responsible for the disclosure should send back the information requested that is

not restricted and attach a note stating: "The information requested is restricted at the request of the individual."

Termination of a restriction

1. An individual will submit in writing a request to terminate a restriction. If the individual orally agrees to terminate a restriction, the termination must be documented in the individual's record.
2. The individual will be informed in writing of the termination of a restriction.
3. Any PHI created or received after written notification of termination is not subject to the restriction.

Confidential communications

1. Reasonable requests to receive communications related to restricted PHI by alternative means or at alternative locations will be honored.
2. The individual must submit the request for confidential communication in writing (either by email or hard copy).
3. Heritage will not honor a request for confidential communication unless it has:
    a. Information as to how payment, if any, will be handled
    b. Specific alternative address or other method of contact
4. An explanation cannot be required as a condition of providing communications on a confidential basis.
5. If confidential communication is requested, the request and approval should be noted by a colored sticker on the client record stating "Confidential Communication Requested." Electronic records should have a field that flags the record as one on which the client has requested confidential communication. Prior to contacting the client, all employees should check to see if confidential communications have been requested.

    The following questions should be asked:
    a. Is confidential communication requested?
    b. Is an alternative address to be used for communication?
    c. Can postcards or letters identifying the organization be sent to the alternative address?
    d. If the address is not restricted, can postcards or letters that identify the agency be sent to the primary address?
    e. Is an alternative telephone number to be used for communication?
    f. Are there times of day in which we are restricted from calling the client?
    g. Can a message be left? Can the message list the name of the agency? Should a blind message with telephone number only be used?

Request to Restrict Use and Disclosure of Protected Health Information

_____, (Print name of Client/guardian/personal representative requesting a specific restriction of PHI.)

To whom does restriction apply? _____

Specific Restriction Requested:

In case of an emergency, this restriction will not be honored.

Client's Signature _____ Date _____

Termination of Restriction

The termination of this restriction must be made either orally or in writing to (entity)

_____.

Client's signature to terminate restriction _____ Date _____

☐ Copy of termination of restriction sent to client on (date) _____

Associated policy: Request to Restrict Use and Disclosure of PHI

Request for Alternative Means or Locations of Communication

Client Information:

Date of Request _____ Client No. _____

Name _____ Date of Birth _____

Address _____

_____

Request for Alternative Communications:

I request Heritage Area Agency on Aging to contact me in/at the following manner:

_____ Telephone communication at the following telephone number _____
_____ Leave message on answering machine
_____ Do not leave message on answering machine

_____ Mail to be sent to the following address:
_____
_____

_____ Other
_____
_____

I further understand that Heritage Area Agency on Aging 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 Client or Legal Representative *Date*

_____ _____
Printed Name *Relationship of Representative to Client*

Health Care Provider:

_____ Accept request for alternative communication

_____ Reject request for alternative communication. Reason for rejection and attached written statement of rejection given to Client.

_____
Name of Staff Processing Request *Date*

Policy 7
Access by Individuals to Protected Health Information

Policy:

Heritage Area Agency on Aging will protect and honor the individual's right to inspect and obtain a copy of PHI in a designated record set for as long as the PHI is maintained in the designated record set. Exceptions to this are:

- Psychotherapy notes
- PHI expected to be used in a civil, criminal or administrative action or proceeding
- PHI maintained that is subject to CLIA amendment of 1988, 42 USC §263a to the extent the provision of access would be prohibited by law or that is exempt from CLIA pursuant to 42 C.F.R. §493.3(a)(2).

Heritage may deny an individual access without providing an opportunity for review in the following cases:

- If an individual is part of a research study, the study is ongoing and they have agreed to the denial of access when they consented to participate in the research and have been informed the right of access will be reinstated upon completion of the research.
- If PHI is subject to the Privacy Act, 5 USC 552a*, provided the denial of the access meets the requirements of the law. (Excerpt from Privacy Act 5 U.S.C. 552a*:* "Nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.")
- If the PHI was received from someone other than a health care provider under a promise of confidentiality and access would be reasonably likely to reveal the source of the information.

Heritage may deny access, provided the individual is given a right to have such denials reviewed, in the following cases:

- If a licensed health care professional has determined that access requested is reasonably likely to endanger the life or physical safety of the individual or another person.
- If PHI makes mention of another person and a licensed health care professional has determined that the access is reasonably likely to cause substantial harm to that other person.
- If the request for access is made by the individual's personal representative and a licensed health care professional has determined that the provision of access is reasonably likely to cause substantial harm to the individual or another person.

Procedure:

I. Individual's request for Access:
   1. The individual must request access to inspect or obtain a copy of the PHI in writing.
   2. A response must be acted on within 30 days after receipt of the written request.
   3. If the individual requests PHI that is not available, but there is knowledge where this information is available at another covered entity, the individual will be informed of the location of the requested PHI.

II. When access is denied:

1. When access to the requested PHI is denied, in whole or in part, a written denial is provided to the individual.
2. The written denial will include the basis for denial, if applicable, a statement of the individual's appeal rights, and an explanation of the process for submitting complaints to Heritage and or to the Secretary of the Department of Health and Human Services. The explanation must include the name, title and telephone number of the Complaint Officer.
3. If the individual has requested a review of a denial, a licensed health care professional will be designated by Heritage to act as a reviewing official. This professional will not have participated in the original decision to deny.
4. The review process will be conducted in a reasonable period of time.
5. Heritage will comply with the decision of the reviewing licensed health care professional.
6. A prompt notice of the review process will be provided to the individual.
7. If the denial decision is rescinded, the time frames for providing access to the requested information apply as outlined in section III of this procedure will apply.

III. When access is granted in whole or in part:
1. The individual will be informed in writing of the decision to allow access.
2. The Individual will be allowed access to the requested PHI within 30 days after receipt of the request. If the information requested is not easily available, the individual will be provided with a written request for a 30-day extension and an explanation for the extension.
3. Access to requested PHI will be limited to the requested information in the designated record set. If the requested information is maintained in more than one designated record sets, there is no need to allow access to the other designated records sets that contain this requested information.
4. A copy of the requested PHI will be given to the individual in the format requested provided a copy can be reasonably made. A readable hard copy or another format will be provided if the requested format is not easily available.
5. Notwithstanding (4), above, if the PHI that is requested by the individual is maintained in one or more designated record sets electronically and if the individual requests an electronic copy, the individual must be provided access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such format or if not, in a readable electronic form and format as agreed to by Heritage and the individual.
6. If the individual agrees in advance, a summary of the requested PHI may be given instead of the actual copy of the PHI. This summary will be in the requested format provided the request can be reasonably accommodated.
7. If the individual's request for access directs Heritage to transmit the copy of PHI to another person designated by the individual, Heritage must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual and clearly identify the designated person and where to send the copy of PHI.
8. The individual will be informed of the fees for each format. Fees will be determined based upon agency cost of supplies, labor, postage, and preparation time when appropriate.

IV. Documentation:

1. A list of designated record sets that are subject to access by individuals will be maintained in the policy manual.
2. The Complaint Officer will maintain a copy of all communication in a file and kept as long as the individual's record is kept or up to 6 years, whichever is the longer amount of time.
3. The Complaint Officer will maintain a record of all decisions regarding access and denial of requests for PHI. This record will be retained as long as the individual's record is maintained or up to 6 years, whichever is the longer amount of time.

Related forms or policies:

1. Client Request for Access to PHI
2. Notice of Decision
3. Request for Appeal/Review of Denial Decision

*Excerpt from the Privacy Act, 5 U.S.C. §552a: "the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finder or voice print or a photograph."

Client Request for Access to Protected Health Information

Name of Client _____ Date of Birth _____

Client Identification Number _____ Date of Request _____

I request that Heritage Area Agency on Aging provide me with access to my personal health information as checked below:

Information Requested:

☐ Medical Records
☐ Billing Records
☐ Other _____

I request access to my personal health information covering the dates of _____ through _____.

Access Requested:

Copies of requested information

Please specify the format you desire

☐ Electronic: _____
☐ Hard Copy: _____
☐ Other: _____

I understand that Heritage Area Agency on Aging may charge a fee for the costs of copying, mailing, or other supplies associated with my request.

☐ Please mail or e-mail the information to:

☐ Inspection of my health information at Heritage Area Agency on Aging office. Please contact us to arrange a mutually convenient time for inspection.

Heritage Area Agency on Aging at 319-398-5559 or 800-332-5934.

_____

Signature of Client or Client's Authorized Representative *Date*

If signed by the client's representative, please print the name and describe the relationship to the client:

_____

Print Name *Relationship*

NOTICE OF DECISION

Client Name and Address

Explanation of Decision:

Your request to access your personal health information as checked below:
☐ Medical Records ☐ Billing Records ☐ Other: _____
_____

For personal health information covering the dates of_____ through _____

In the format of:
☐ Copies of requested information at the cost of $_____

☐ Inspection of my health information at Heritage Area Agency on Aging

Has Been:
☐ **Accepted.** Please make arrangements by calling Heritage Area Agency on Aging at 319-398-5559 or 800-332-5934. You may also come to the Heritage Main Office located on the Kirkwood Community College campus, 6301 Kirkwood Blvd. SW, Cedar Rapids, IA. You will be given a date and time for which you can inspect your personal health information or receive copies if that is your choice. See cost of copies above.

☐ **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.
☐ The information is related to a civil, criminal, or administrative action.
☐ The information is subject to or exempt from the Clinical Laboratory Improvement Amendments of 1988 (CLIA).
☐ You are an inmate and the information 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 research.
☐ The information is subject to the Privacy Act.
☐ The information requested was obtained from a third party (non-health care provider) under condition of confidentiality.

You do not have an opportunity to request a review of Heritage's decision in these circumstances.

OR

Your request has been denied for the following reason:

☐ A licensed health care professional has determined that the access requested is likely to endanger the life or physical safety of yourself or others and/or the information 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 information 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 _____
_____
_____

You may request a review of this decision by completing the appeal form.

Staff Signature _____ Date _____

Request for Appeal/Review of Denial Decision

If you have been denied a request to access your protected health information, you may ask for an appeal or review of that denial:

1. To request a review or appeal, complete the form below and submit to: Complaint Officer, at Heritage Area Agency on Aging within 10 working days of receipt of the denial notice. The review will be held in private. 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 Iowa Legal Aid for assistance.

2. A written notice will be issued within 10 working days informing you of the date, time, place, and name of the Licensed Healthcare Professional who will conduct the review.

3. A written decision will be issued no later than 10 working days after the review is heard. A copy of the decision will be sent to you by certified mail.

Request for Appeal/Review of a Denial

☐ I request review of the denial decision.

_____

Individual's Signature *Date*

Policy 8
Amendment of Protected Health Information

Policy:

An individual has the right to request an amendment of protected health information or a record about the individual in a designated record set as long as the protected health information is maintained in the designated record set.

Heritage Area Agency on Aging may deny an individual's request for amendment if a determination is made that the protected health information or record that is the subject of the request:

1. Was not created by Heritage, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
2. Is not part of the designated record set;
3. Would not be available for inspection under policy of access of individuals to protected health information or has been denied access; or
4. Is accurate and complete.

Procedure:

Requests for amendment are to be in writing and should include a reason for the requested amendment.

Heritage Staff and Subcontracting Staff Roles:

1. Heritage Staff will assist any client requesting a primary correction to his or her record to complete the Request for Amendment/Correction of PHI Form. A primary correction would include *improperly* noted diagnosis or other *improperly* noted item that causes distress to the client. This procedure would not be necessary or practical in the case of a secondary clerical error such as the transposing of numbers in a telephone number or address, punctuation, other non-medical or non-care related clerical corrections or updates.
2. Heritage Staff will bring any such requests to the attention of the Privacy Officer for review.
3. The Privacy Officer will provide a copy of any requests to the Heritage Privacy Officer.

Timely action: An individual's request for an amendment will be acted on no later than 60 days after receipt of such a request.

1. If Heritage is unable to act on the amendment within 60 days of receipt of the written request, a 30 day extension is permitted, provided that:
    A. Heritage, within the 60 day time limit, 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 date of request; and
    B. Only one such extension of time is permitted for action on a request for an amendment.

Accepting the amendment: When accepting the requested amendment, in whole or in part:

1. Identify the records in the designated record set that are affected by the amendment and append or otherwise provide a link to the location of the amendment.

2. Inform the individual that the amendment is accepted.
3. Obtain the individual's identification of and agreement to notify the relevant persons with whom the amendment needs to be shared.
4. Efforts will be made to inform and provide the amendment within a reasonable time to:
    A. Persons identified by the individual as having received protected health information about the individual who need the amendment.
    B. Persons including business associates that Heritage knows have the protected health information that is the subject of the amendment and that may have relied on or could foresee ably rely on such information to the detriment of the individual.
5. Subcontracting Care Program Team Members will provide Heritage a copy of any completed Request for Amendment/Correction of PHI Forms and copies of any amended/corrected documents for the Master Chart.

Denying the amendment: When denying the requested amendment, in whole or in part:

1. Provide the individual with a written denial no later than 60 days after the written request was received. The denial must use plain language and contain:
    A. The basis for the denial. (See policy statement for criteria)
    B. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.
    C. A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment.
    D. A description of how the individual may submit a complaint pursuant to the agency complaint procedures or to the Secretary of the Department of Health and Human Services. The description must include the name or title and telephone number of the contact person.
2. Permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. Heritage may reasonably limit the length of a statement of disagreement.
3. If deemed appropriate, a written rebuttal to the individual's statement of disagreement may be prepared by Heritage. If a rebuttal is prepared, a copy will be given to the individual who submitted the statement of disagreement.
4. Identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the rebuttal, if any, to the designated record set.
5. Future disclosures:
    A. If a statement of disagreement has been submitted by the individual, Heritage will include the material appended in accordance with paragraph 4 of this section, or an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.
    B. If the individual has not submitted a written statement of disagreement, Heritage will include the individual's request for amendment and its denial or an accurate summary of such information with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with #1 (C) of the denial section (above).

C. When a subsequent disclosure involves using a standard transaction that does not permit the additional material to be included with the disclosure, the appended information will be submitted separately.

Action on Notices of Amendment: When informed by another covered entity of an amendment to an individual's protected health information Heritage will:

1. Amend the protected health information in designated record sets it maintains as provided in the section titled Accepting the Amendment paragraph 1.
2. Document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation following agency policy for record retention.

Request for Amendment/Correction of Protected Health Information

Client Name: _____ Request Date: _____
Street Address: _____ Birth Date: _____
City/State/Zip: _____ MR/Account # : _____

What Needs to be Amended/Corrected & Why

Entry to be amended: _____
Date & Author of entry: _____

Please explain how the information is incorrect or incomplete. What should the information state to be more accurate or complete?

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

Names & Addresses:

I understand that the provider may or may not amend the medical record with an amendment based on my request, and under no circumstances is the provider permitted to alter the original medical record. In any event, this request for an amendment will be made part of my permanent medical record.

_____
Signature of Client or Client's Legal Representative *Date*

_____
Representative Capacity

For Healthcare Organization/Internal Use Only

Date Received: ☐ Accepted ☐ Denied

If denied, check reason for denial:

☐ PHI was not created by this organization
☐ PHI is not available to the Client for inspection as permitted by federal law (e.g., psychotherapy notes)
☐ PHI is not part of client's designated record set
☐ PHI is accurate and complete

Comments:

☐ Individual was informed of denial in writing (attach letter of communication)

_____
Signature/Title of Team Member *Date*

Policy 9
Accounting of Disclosures of Protected Health Information (PHI)

Policy:

An accounting of disclosures will be kept in each client record and be completed by any employee who discloses protected health information from the clinical record. Protected health information is information including demographic information that may be used for identification of individuals that relates to past, present or future physical or mental health condition and related health care services. A disclosure refers to the release, transfer or other conveyance of protected health information outside the entity holding information. The accounting of disclosures provides a complete and accurate account of all disclosures of protected health information made by the covered entity and business associates, with exceptions.

The exceptions or instances where a covered entity is not required to account for disclosures, include:

- disclosures made by the covered entity to carry out treatment, payment, or health care operations
- disclosures to individuals about themselves
- disclosures occurring prior to July 1, 2006
- disclosures made that only contain de-identified health information for statistical use (information that cannot identify an individual)
- disclosures resulting from an authorization
- disclosures to persons involved in providing care to the individual
- disclosures provided while the individual is present
- disclosures related to national security or intelligence
- disclosures to correctional institutions or law enforcement officials

Heritage and Subcontracting Staff roles:

1. The Accounting Disclosure Log (p. 37 of the HIPAA Manual) will be copied and attached to every master chart and Heritage Care Program Team Members chart. It should be located in the front most part of the chart directly on top of the Releases of Information.
2. Subcontracting Care Program Team Members shall utilize The Accounting Disclosure Log (p. 37) and Request for Accounting Disclosures (p. 36) as appropriate in their individual agencies.
3. Subcontracting Care Program Team Members must identify individuals in their agency who may be in a position to disclose the information and work with Heritage to ensure those individuals are properly trained in completing such forms.
4. LifeLong Link Team Members will use caution in determining whether the information being requested is covered by a Release of Information and/or by "TPO".
5. Any Requests for Accounting Disclosures submitted to the subcontracting agency shall be filled by the subcontracting agency as appropriate, and a copy of that request shall be sent to Heritage.
6. Upon transfer to another CMPFE entity, Heritage will supply the current case manager with the Request for Accounting Disclosures (p. 36). This must be completed and returned to Heritage before any electronic transfers will be made or before copies are sent from the chart.
7. A copy of any requests will be provided to The HIPAA Privacy Officer at Heritage at which point the letter of accompaniment (p. 38) will be completed and returned to the requesting entity.

Procedure:

1. Upon request, the employee providing the disclosure will complete an accounting of the disclosure. The content of the accounting for each disclosure will include:
    - The date of disclosure.
    - The name of entity or person who received the PHI and, if known, the address and phone number of such entity or person;
    - A brief description of the protected health information disclosed; and
    - A brief statement of the purpose of the disclosure that reasonably informs the individual of the disclosure.

    (See Written Accounting of Disclosures of individual's Protected Health Information form.)
2. The provisions of disclosure without consent of the individual include Census Bureau statistics, National Archives, civil or criminal law enforcement, Congress (oversight capacity), Controller General (GAO activities), court order (signed by judge), consumer reporting agency, and compelling circumstances affecting health or safety of individua1 (must be justified).
3. Multiple disclosures of PHI to the same person or entity for a single purpose will provide the frequency, periodicity, or number of the disclosures made during the accounting and the date of the last such disclosure during the accounting period.
4. The time period for accounting is six (6) years prior to the date of request.
5. Compliance with a request will be granted no later than sixty (60) calendar days after receipt of the request. If unable to take action on the request within the 60-day period, the time frame may be extended by no more than thirty (30) calendar days. Notification of the extension will be provided within the original sixty (60) day period the individual will be provided with a written statement of the reason(s) for the delay and the date by which the agency will provide the accounting. Only one such extension will be permitted on a request.
6. The individual will be notified in advance of the fee for the disclosure accounting. The first accounting to an individual in any 12-month period will be granted without charge. A reasonable cost-based fee will be assessed for each subsequent request for an accounting if during the same 12-month period.
7. All documentation related to the accounting of disclosures of PHI will be retained for six (6) years from the date of its creation or from the date when it was last in effect, whichever is later.

Related forms or policies

- Request for Accounting of Disclosures form
- Reply letter form
- Accounting Disclosure Log

Request for Accounting of Disclosures

Client Information:

Date Requested: _____ Client Number: _____

Name: _____ Date of Birth: _____

Address: _____

_____

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 July 1, 2006.

From: _____ To: _____

I request the accounting to be sent to the following address (if different from above):

_____

_____

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 $_____. I understand that there is (check one):

_____ No fee for this request.

_____ A fee for this request in the amount specified above and I wish to have an accounting prepared.

I understand the accounting I have requested will be provided to me within 60 days unless I am notified in writing that an extension of up to 30 days is needed.

_____

Signature of Client or Legal Representative *Date*

_____

Representative Capacity

Heath Care Provider Information:

Date request received: _____ Date Accounting Sent: _____

Extension requested: _____ Yes _____ No

If yes, give reason:

_____

_____ Client notified in writing of extension (attach copy of notice of reasons for delay and date for provision of accounting).

Name of Staff Member Processing Request: _____

Accounting Disclosure Log

Client Name: _____ Client Number: _____

Date Request Received	Person Making Request	Date of Disclosure	Name & Address of Recipient of PHI	Description of PHI Disclosed	Purpose of Disclosure (or Copy of Written Request)	Name of Staff Processing Request

Dear ,

The accounting you requested on ___/___/___ of the disclosures of your protected health information that our agency or our business associates made within the six years before your request has been prepared. The charge for disclosure is $ _____. Upon receipt of payment, we will send the disclosure accounting to you.

The disclosure accounting does not include disclosures we or our business associates made before July 1, 2006, which is our compliance date under federal privacy rules. The disclosure accounting also does not include disclosures made to carry out your treatment, payment for treatment, or health care operations, disclosures made to you or to your personal representatives and others involved in your health care or payment for your health care. We are not required to account for these disclosures.

For each accountable disclosure, we have provided:

- The date
- The name and, if known, the address of the person or entity to which the disclosure was made
- A description of the protected health information disclosed
- The purpose for which the protected health information was disclosed.

If you have questions regarding the disclosure accounting, please contact the Privacy Officer of Heritage Area Agency on Aging at the address or telephone listed.

Sincerely,

Heritage Area Agency on Aging

Privacy Officer Signature

Policy 10
Other Requirements Relating to Uses and Disclosures of Protected Health Information 164.514

Policy:

To ensure the confidentiality of individual Protected Health Information (PHI), Heritage Area Agency on Aging will comply with the Privacy Standards for De-Identification, Minimum Necessary, Limited Data Set, Fundraising and Verification as outlined in the Health Insurance Portability and Accountability Act of 1996.

Procedure:

I. De-Identified Information

Heritage may de-identify health information so that it is no longer PHI. To do so, identifiers of the individual, or relatives, employers or household members must be removed. Those identifiers are:

- Names
- Address, City, County, Precinct
- Zip Code (other than the first 3 digits)
- Dates (other than year)
- Telephone Numbers
- Fax Numbers
- Vehicle Identifiers
- Device Identifiers and Serial Numbers
- Internet Protocol Address Number
- Web Universal Resource Locators (URLs)
- Other Identifying Number, characteristic or code
- Electronic Mail Addresses
- Social Security Numbers
- Medical Records Numbers
- Health Plan Beneficiary Numbers
- Account Numbers
- Certificate/License Numbers
- Photographic Images
- Biometric Identifiers

A code or other means of record identification may be assigned to allow de-identified information to be re-identified by Heritage, provided that the code is not easily translated so as to identify the individual. In addition, neither the code nor the mechanism for re-identification will be disclosed.

II. Minimum Necessary

Any request for PHI will be limited to that which is reasonably necessary to accomplish the purpose for which the request is made. Persons or classes of persons are identified as appropriate to access PHI to carry out their duties. For each person or class of persons, the category or categories of PHI to which access is needed is identified along with the conditions appropriate for such access. Reasonable efforts will be made to limit the access of each person or class of persons.

For all uses, disclosures and requests, an entire medical record will not be disclosed unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

For any type of disclosure made on a routine and recurring basis, procedures will limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

Standards to consider when complying with a request for PHI:

1. Each request for disclosure shall be evaluated on an individual basis.
2. Determine if the information meets the purpose of the request.
3. Determine the minimum necessary to meet the purpose of the request.

The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment;
- Uses and disclosures made to the individual;
- Uses or disclosures made pursuant to an authorization;
- Disclosures made to the Secretary of Health and Human Services to determine compliance, or
- Uses or disclosures that are required by law, including, compliance with HIPAA privacy provisions.

Other Disclosures

Criteria is available for all other disclosures. These criteria will limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure and review requests for disclosure on an individual basis. Requested disclosure may serve as the minimum necessary, if that is reasonable, under the following circumstances:

1. Disclosures made to public officials pursuant to 164.512, if the public official represents that the requested information is the minimum necessary;
2. Information requested by another covered entity;
3. Information requested by a professional who is a member of the workforce or is a business associate of Heritage Area Agency on Aging for purposes of providing professional services to the organization, if the professional represents that the information requested is the minimum necessary for the stated purpose.
4. For purposes of research when documentation or representations comply with 164.512 (I).

III. Limited Data Set

A limited data set is PHI that excludes the certain direct identifiers of the individual or of relatives, employers, or household members of the individual. If a data use agreement is entered into, a limited data set may be disclosed that meets the requirements of the agreement.

The Limited Data Set excludes the following:

Names
Postal address information (other than town or city, state, or zip code)
Telephone numbers
Fax numbers
Electronic mail addresses
Social Security Number
Medical record numbers
Health plan beneficiary numbers
Account numbers
Certificate/license numbers
Account numbers
Vehicle identifiers and serial numbers, including license plate numbers
Device identifiers and serial numbers
Web Universal Resource Locators (URL's)
Internet Protocol (IP) address numbers

Biometric identifiers, including finger and voiceprints
Full face photographic images and any comparable images

Permitted purposes for uses and disclosures of limited data sets:

- Research
- Public health
- Health care operations
- A business associate

IV. Fundraising and PHI

For purpose of raising funds for its own benefit, the following PHI may be used or disclosed to a business associate or institutionally related foundation without an authorization:

- Demographic information related to the Client; and
- Dates of health care provided to the Client.

An authorization will be obtained from the Client to use or disclose PHI beyond the uses and disclosures stated above.

The Notice of Privacy Practices includes a statement that the client PHI may be used for fundraising activities unless the client objects to this use.

Fundraising communications will include a statement informing the recipient that he or she may opt out of future fundraising communications with a description of how to do so.

Heritage will maintain a log of all clients and others who have opted out of receiving future fundraising communications. Reasonable efforts will be made to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

V. Verification

Care will be taken to verify identification of a person requesting PHI and the authority of such person to have access to PHI if the identity or authority of the person is not known to anyone at Heritage. This can include oral or written verification. Verification may be satisfied by, for example, an administrative subpoena or a written statement that demonstrates that the requirement has been satisfied. Documentation must be signed and dated.

Verification of identity may be satisfied by the following when the disclosure is requested by a public official:

1. If the request is made in person, presentation of an agency identification badge or other official credentials;
2. If the request is in writing, the request should be on appropriate government letterhead or a written statement of legal authority. A written statement of legal authority can include a subpoena or warrant.
3. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority.

Standards to consider when complying with verification of identity:

1. Obtain written documentation of the verification.
2. If written documentation is not available, document the oral communication verifying the identity of the individual requesting the disclosure.
3. Documentation that the individual requesting the disclosure is known by someone in the organization if no other verification is required.

Related policies/procedures

1. Workforce Designation Procedure

Workforce Designation-Minimum Necessary Form

Date: _____ _____

Signature of Privacy Officer or Designee

Identify those persons or classes of persons, as appropriate, in the workforce who need access to protected health information to carry out their duties.

For each such person or class of persons, identify the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

Position/Job Title	Need Access to PHI to Perform Job Yes/No	Category(ies) of PHI to be Accessed	Method of Access to PHI
Executive Director	**Yes**	**All**	**Any**
Privacy Officer	**Yes**	**All**	**Any**
Fiscal Director	**Yes**	**All**	**Any**
Data Management Team	**Yes**	**All**	**Limited**
Finance Team Members	**Yes**	**All**	**Any**
Care Team Members	**Yes**	**Program specific**	**Any**
Program Staff	**Yes**	**Program specific**	**Limited**

Policy 11
Reporting Compliance Concerns

Policy:

Heritage Area Agency on Aging believes that an effective system of communication is important in identifying compliance violations of the privacy standards to protect the health information created or received. To encourage communication of compliance concerns by members of the workforce and other agents doing business with us, Heritage 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.

Heritage will make every reasonable effort to protect the identity of a reporting employee, unless the employee permits his or her identity to be revealed. No disciplinary action or retaliation will be taken against an employee who makes a good faith report of a compliance concern. Any individual who retaliates against an employee for reporting a compliance concern will be subject to disciplinary action, up to and including termination.

Sanctions:

- Heritage will apply appropriate sanctions against members of the workforce who fail to comply with the privacy policies and procedures of the agency. All sanctions will be documented on disciplinary action forms and will follow disciplinary action guidelines.
- A member of the workforce who shares protected health information will not be subject to sanctions by reporting what they believe to be a violation by the agency.

Mitigation:

- Ensure reasonable mitigation, if protected health information is disclosed in violation of these policies and procedures.
- The agency may not intimidate, threaten, coerce, discriminate against, or take retaliatory action against:
    1. Any individual or person filing a complaint
    2. Any individual or member of the workforce testifying, assisting, or participating in an investigation, compliance review proceeding, or hearing.
    3. Any individual or member of the workforce who reports what they believe, in good faith, to be a violation of HIPAA standards.

Waiver of Rights

The agency may not require individuals to waive their rights as a condition of the provision of treatment or payment.

Procedures:

<u>Report of Concern</u>

A report of concern may be made by anyone having knowledge or information about a known or suspected violation of the privacy standards or the laws and regulations governing Heritage. Reports may be made verbally or in writing to the Privacy Officer. All reports, whether verbal or written, will be documented on the *Confidential Report of Concern.*

Reporting System

Reports of compliance concerns can be made in any one of the following ways:

1. Verbal report by a named individual, in person or by telephone, made to the Privacy Officer.

2. Written report by a named individual, by use of the *Confidential Report of Concern*, submitted to the Privacy Officer.

3. Anonymous telephone report by an unidentified individual made to the Privacy Officer.

4. Anonymous written report by an unidentified individual, by use of the *Confidential Report of Concern*, mailed to the Privacy Officer at the organization's address.

Investigation of Reports

The Privacy Officer will investigate each report of concern. The findings of an investigation prompted by a report of concern will be recorded on the *Compliance Report Investigation Form* within five working days of the report. All findings will be shared with the Heritage Board of Directors at the earliest opportunity.

Confidential Report of Concern

The purpose of this form is to report the facts pertaining to any known or suspected violation of Heritage Area Agency on Aging's privacy standards or the laws and regulations governing Heritage. 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 either mailing it or delivering it to the Privacy Officer at the organization's address.

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 do not call, the Privacy Officer will not be able to report back the outcome of the investigation arising out of your report.

If you wish to identify yourself in this report, Heritage will make every effort to keep your identity confidential, unless you give Heritage 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 Heritage's privacy standards occurred. Please include a copy or a description of any documents that support your concerns.

Reference number: _____

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, & places):

_____

_____

_____

_____

_____

_____

Name(s) of person(s) involved in the incident and an explanation of the person's:

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).

Policy 12
Privacy and Complaint Officer

Policy:

Heritage Area Agency on Aging is considered a covered entity as a health care provider by its governing board for certain of its HIPAA-covered programs. The Privacy Officer will be the employee of the Agency who is responsible for the development and implementation of the policies and procedures. The Privacy Officer of the Agency will be the contact person who is responsible for receiving complaints and providing further information about HIPAA related issues.

Privacy and Complaint Officer Job Description:

General Purpose: The privacy and complaint officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the privacy of, and access to, Client health information in compliance with federal and state laws and the organization's information privacy practices.

Responsibilities of Privacy Officer:

- Provides guidance and assists in identification, implementation, and maintenance of privacy policies and procedures.
- Coordinates with the agency management team, legal counsel, and the Advisory Council any appropriate issues.
- Works with agency staff to establish a privacy oversight committee as necessary.
- Performs initial and periodic privacy risk assessments and conducts related ongoing compliance monitoring activities with the partnership and cooperation of the Care Connections Director.
- Works with appropriate personnel to assure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, information notices, and materials, reflecting current organization and legal practices and requirements.
- Ensures delivery and documentation of initial privacy training and orientation to all staff and appropriate volunteers.
- Work with business associates to ensure privacy concerns, requirements and responsibilities are addressed.
- Will maintain a mechanism to track access to protected health information as required by law. Qualified individuals would be allowed to review or receive a report on such activity.
- Works cooperatively with appropriate personnel in overseeing Client rights to inspect, amend, and restrict access to protected health information when appropriate.
- Ensures application and documentation of sanctions for failure to comply with privacy policies for all workforces in cooperation with appropriate administrative personnel and legal counsel as applicable.
- Initiates, facilitates and promotes activities to foster information privacy awareness within the agency and related entities.
- Works with all Agency workforce involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the organization's policies and procedures and legal requirements.

- Maintains current knowledge of applicable federal and state privacy laws to ensure organizational adaptation and compliance.
- Serves as information privacy consultant to the agency for all departments and appropriate entities.
- Cooperates with the Office of Civil Rights, other legal entities, and agency officers in any compliance reviews or investigations.
- Will ensure that all current workforce will be trained according to HIPAA guidelines. Those hired after initial training will have two months to receive required training.

Qualifications:

- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
- Demonstrated organization, facilitation, communication, and presentation skills.

Responsibilities of Complaint Officer:

- Responsible for receiving, documenting, tracking, investigation, and taking action on all complaints regarding privacy policies and procedures and will seek legal counsel when necessary.
- Will assure compliance with complaint policy and process.
- The agency Disciplinary Action Policy will be used, and HIPAA related issues will be referred to the HIPAA Privacy and Complaint Officer.

Qualifications:

- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
- Demonstrated organization, facilitation, communication, and presentation skills.

Policy 13
HIPAA Violation Sanction Policy

In the event, that you as an employee of Heritage Area Agency on Aging are responsible for a Violation of the agency's Privacy Practices and/or violate the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the following sanction guideline would apply:

Definition of Offense:
Class I Offenses:

1. Accessing information that you do not need to know to do your job;
2. Sharing your computer access codes (user name & password);
3. Leaving your computer unattended while you are logged into a PHI program;
4. Sharing PHI with another employee without authorization;
5. Copying PHI without authorization;
6. Changing PHI without authorization;
7. Discussing confidential information in a public area or in an area where the public could overhear the conversation;
8. Discussing confidential information with an unauthorized person; or
9. Failure to cooperate with Privacy Officer

Class II Offenses:

1. Second offense of any class I offense (does not have to be the same offense);
2. Unauthorized use or disclosure of PHI;
3. Using another person's computer access codes (user name & password); or
4. Failure to comply with a team resolution or recommendation.

Class III Offenses:

1. Third offense of any class I offense (does not have to be the same offense);
2. Second offense of any class II offense (does not have to be the same offense);
3. Obtaining PHI under "false pretenses"; or
4. Using and/or disclosing PHI for commercial advantage, personal gain or malicious harm.

Sanctions:
Class I offenses shall include, but are not limited to:

a. Verbal reprimand;
b. Written reprimand in employee's personnel file;
c. Retraining on HIPAA Awareness;
d. Retraining on Agency's Privacy Policy and how it impacts the employee and employee's department; or
e. Retraining on the proper use of internal forms and HIPAA required forms.

Class II offenses shall include, but are not limited to:

a. Written reprimand in employees personnel file;
b. Retraining on HIPAA Awareness;
c. Retraining on Agency's Privacy Policy and how it impacts the employee and employee's department;
d. Retraining on the proper use of internal forms and HIPAA required forms; or
e. Suspension of employee (in reference to suspension period: minimum of one (1) day; maximum of three (3) days).

Class III offenses shall include, but are not limited to:

a. Termination of employment;
b. Civil penalties as provided under HIPAA or other applicable Federal/State/Local law; or
c. Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law.

Acknowledgment:

I, the undersigned employee, hereby acknowledge receipt of a copy of the HIPAA Violation Sanction Policy for Heritage Area Agency on Aging. Dated this _____ day of _____ 20___.

_____

Signature of Employee

Policy 14
Training

Policy:

Heritage Area Agency in Aging will provide training to its employees in an effort to comply with the Privacy Rule of HIPAA's Administrative Simplification provisions.

Procedure:

Heritage will train all of our staff employed. New employees will be trained on HIPAA within 60 days of employment. Whenever there are material changes to our privacy practices, the Privacy Officer will determine the employees affected by the change and coordinate the training of those employees. Training regarding material changes to our privacy practices will take place within 30 days after the implementation date for the changes.

Heritage will maintain documentation regarding the content and those in attendance at any HIPAA training. Copies of all attendance sheets, handouts, slides, curriculum and evaluations will be kept in the files of the Privacy Officer for six years from the date of the training. Employees who fail to attend training will be subject to discipline for breach of privacy practices.

Each training will include information on how to contact the Privacy Officer and where to get additional information.

Trainings can be through workshops, self-study and staff meetings. The Privacy Officer is encouraged to develop on-going reminders of the agency's privacy practices through poster campaigns, memos and newsletters.

Training Documentation
Heritage Area Agency on Aging

I acknowledge that I received training regarding the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition, I acknowledge that I have a general understanding:

1. Of the core elements of HIPAA,
2. Of how to contact Heritage Area Agency on Aging Privacy Officer,
3. Of Heritage Area Agency on Aging HIPAA Privacy Policies and Procedure, and
4. Of Heritage Area Agency on Aging Information Security Policy.

Signature of Employee

Printed Name of Employee

Position

Date of Training

Provided Training

Policy 15
Business Associates

Policy:

In an effort to comply with the Privacy Rule of HIPAA's Administrative Simplification provisions, Heritage Area Agency on Aging will enter into Business Associate Agreements with certain third parties.

Procedure:

The agency will determine if each vendor or independent contractor is a Business Associate. It will consider any vendor or independent contractor a Business Associate if the following characteristics exist:

1. The vendor or independent contractor performs a function or activity on behalf of Heritage that involves the creation, use, disclosure or maintenance of PHI or provides any legal, actuarial, accounting, consulting, data aggregation or management, administrative, accreditation, or financial services to or for us where the provision of the service involves the disclosure of individually identifiable health information from such covered entity to the vendor or independent contractor;
2. The vendor or independent contractor is <u>not</u> involved in the treatment of a client;
3. The vendor or independent contractor is <u>not</u> providing consumer-conducted financial transactions.

Any vendor or independent contractor who qualifies as a Business Associate will be required to sign a Business Associate Agreement. The Agreement will be in the form attached to this policy. Amendments to the Business Associate Agreement will not be made without the approval of legal counsel.

The Privacy Officer working with the Executive Director and legal counsel will develop and maintain a list of the Agency's Business Associates. Staff will report to the Privacy Officer any time they are considering the development of a business relationship with another individual or organization that will use PHI created or disclosed by the agency to conduct agency-related work.

Prior to signing a contract with a Business Associate, the Privacy Officer will assign a risk level to the contractual relationship. High-risk contracts are those in which Business Associates have access to client databases and medical records, for example, outside utilization managers, software vendors or consultants. Medium risk contracts are those in which the Business Associate has limited access to client databases and/or medical records, for example, third-party billing companies. Low risk contracts are those in which the Business Associate has limited access to client databases and/or medical records, for example, accountants who infrequently need PHI in order to do work for the Agency.

If, at any time, a staff person becomes aware that a Business Associate is in breach of its Business Associate Agreement, the employee should contact his or her supervisor or the Privacy Officer. Breach can include security lapses, privacy violations and failure to cooperate with Heritage in complying with its obligations, such as accounting for disclosures of PHI or giving individuals access to their PHI.

Any report by a Business Associate of any breach of its Business Associate Agreement or our privacy policies should be immediately forwarded to the Privacy Officer. The Privacy Officer will be responsible

for logging any reported breach and any follow up. If the Privacy Officer believes that a Business Associate has materially breached the agreement or has been reported for a number of smaller breaches that cause the Privacy Officer to be concerned about the Business Associate's ability to perform in compliance with the agreement, the Privacy Officer, after consulting with the Executive Director and Heritage's legal counsel, can terminate the contractual relationship with the Business Associate.

Upon termination of the Business Associate Agreement, the Business Associate will destroy or return the PHI it is maintaining, using or storing on behalf of the Agency. The Privacy Officer will be responsible for overseeing the orderly transfer or destruction of the PHI and for assuring the Business Associate's compliance with any post-contract obligations.

HERITAGE AREA AGENCY ON AGING
BUSINESS ASSOCIATE AGREEMENT

This Agreement is effective on July 1, 2014 through June 30, 2015, between Heritage Area Agency on Aging (Covered Entity") and _____ ("Business Associate"). Covered Entity and Business Associate enter into this Agreement in order to comply with the administrative simplification requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), set forth in Title 45, Parts 160 and 164 of the Code of Federal Regulations ("CFR"), the Health Information Technology for Economic and Clinical Health Act and its implementing regulations and the HIPAA Privacy, Security, Enforcement and Breach Notification Omnibus Final Rule.

I. Definitions

Definitions. Capitalized terms not otherwise defined in the Agreement shall have the meanings given to them in Title 45, Parts 160 and 164 of the CFR and are incorporated herein by reference.

II. Obligations and Activities of Business Associate

Prohibition on Unauthorized Use or Disclosure of PHI. Business Associate shall not use or disclose any protected health information ("PHI") received from or on behalf of Heritage, except as permitted or required by this Agreement, as necessary to perform the services set forth in an underlying services agreement with Heritage, as required by law or as otherwise authorized in writing by Heritage.

Appropriate Safeguards. Business Associate shall develop, implement, maintain, and use appropriate safeguards to prevent any use or disclosure of the PHI or Electronic Protected Health Information ("EPHI") other than as provided by this Agreement, and to implement administrative, physical, and technical safeguards as required by sections 164.308, 164.310, 164.312 and 164.316 of title 45, Code of Federal Regulations and HITECH to protect the confidentiality, integrity, and availability of EPHI or PHI that business Associate creates, receives, maintains, or transmits, in the same manner that such sections apply to the Covered Entity. See HITECH § 13401.

Breach Notification. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for in the agreement of which it becomes aware, including breaches of unsecured PHI as required at 45 C.F.R. 164.410 and any security incident of which it becomes aware. In the event of such unauthorized use or disclosure, Business Associate shall make a report to Heritage's Privacy Officer less than 24 hours after Business Associate learns of the unauthorized use or disclosure (and in no case later than 5 calendar days after discovery). Business Associate's report shall at least:

1. Identify each individual whose PHI has been, or is reasonably believed by the Business Associate to have been accessed, acquired or disclosed. Identify the nature of the unauthorized use or disclosure, the PHI/EPHI used or disclosed, identify who made the unauthorized use or received the unauthorized disclosure, what Business Associate has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure and what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure. In addition, Business Associate must provide such other information, including a written report, as reasonably requested by Heritage's Privacy Officer, all in accordance with the data breach notification requirements set forth in 42 U.S.C. § 17932 and 45 C.F.R. 164.404(c) and 164.410. In the event notification is required, Heritage shall determine

who (as between Heritage and Business Associate) will be responsible for notification. In all cases, Business Associate shall bear the expense of any required notification and/or any mitigating measures that Heritage deems appropriate in light of the breach.

2. A breach or unauthorized use or disclosure shall be treated as discovered by a Business Associate as of the first day on which such breach or unauthorized use or disclosure is known or should have reasonably been known.

Subcontractors and Agents. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate shall require each of its subcontractors or agents to whom Business Associate may provide PHI received from or created or received by Business Associate on behalf of Heritage to agree to written contractual provisions pursuant to 45 C.F.R. 164.308(b)(1) and HITECH § 13401 that impose at least the same obligations to protect such PHI as are imposed on Business Associate by this Agreement.

Access to PHI. Business Associate shall provide access, at the request of Heritage, to PHI in the Designated Record Set to Heritage or, as directed by Heritage, to an Individual in order to meet the requirements under 45 C.F .R. 164.524 and applicable state law. Business Associate shall provide access in the time and manner set forth in Heritage's health information privacy and security policies and procedures. Business Associate also agrees to provide Heritage's Privacy Officer access to any information necessary to confirm compliance with the HIPAA privacy regulations.

Amending PHI. Business Associate shall make any amendments to PHI in a Designated Record Set that Heritage directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Heritage or an Individual and in the time and manner set forth in Heritage's health information privacy and security policies and procedures. Business Associate shall take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526.

Accounting of Disclosures of PHI. Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Heritage to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

Within ten (10) days of notice by Covered Entity of a request for an accounting of disclosures of PHI, Business Associate and any agents or subcontractors shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under the Privacy Rule, including but not limited to 45 C.F.R. § 164.528. If the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, if any, Business Associate shall within five (5) business days of such a request notify Covered Entity about such request. Covered Entity shall either request that business Associate provide such information directly to the Individual, or it shall request that the information be immediately forwarded to Covered Entity for compilation and distribution to such Individual. Notwithstanding anything in the Agreement to the contrary, Business Associate and any agents or subcontractors shall continue to maintain the information required for purposes of complying with this Section for a period of six (6) years after termination of the Agreement.

Access to Books and Records. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI/EPHI received from or on behalf of Heritage available to Heritage and to DHHS or its designee for the purpose of determining Heritage' s compliance with the privacy rule.

III. Permitted Uses and Disclosures by Business Associate

Use and Disclosure of Protected Health Information. Business Associate shall use and/or disclose PHI only to the extent necessary to satisfy Business Associate's obligations under this Agreement. Business Associate agrees to use or disclose only the minimum amount of information necessary to accomplish the intended purpose of the request pursuant to 45 C.F.R. §§164.502(b) and 164.514(d), i.e., the minimum amount of information to carry out the use or disclosure requested.

Business Associate's Operations. Except as otherwise limited in this BAA, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Service Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of Covered Entity. Business Associate may use PHI it creates or receives for or receives from Heritage only to the extent necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities. Business Associate may disclose such PHI as necessary for Business Associate's proper management or administration or to carry out Business Associate' s legal responsibilities only if:

(a) The disclosure is required by law; or Business Associate obtains reasonable assurances, evidenced by written contract, from any person or organization to which Business Associate shall disclose such PHI that such person or organization shall:

(i) hold such PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization or as required by law; and

(ii) in the event of a breach of Unsecured PHI, Business Associate shall be notified.

Protection of Exchanged Information and Electronic Transactions. If Business Associate conducts any Standard Transaction for or on behalf of Heritage, Business Associate shall comply and shall require any subcontractor or agent conducting such Standard Transaction to comply with each applicable requirement of Title 45, Part 162 of the CFR. Business Associate shall not enter into or permit its subcontractors or agents to enter into any Trading Partner Agreement in connection with the conduct of Standard Transactions for or on behalf of Heritage that: changes the definition, Health Information condition or use of a Health Information element or segment in a Standard; adds any Health Information elements or segments to the maximum defined Health Information set; uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification or not in the Standard's Implementation Specifications; or changes the meaning or intent of the Standard's Implementation Specifications.

IV. Provision for Covered Entity to Inform Business Associate of Restrictions

Changes in or Restriction to Uses and Disclosures. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to or must comply with in accordance with 45 CFR § 164.522 and/or HITECH § 13405(a).

V. Termination

Termination by Covered Entity for Cause. Upon Heritage's knowledge of a material breach by Business Associate, Heritage shall provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Heritage. Heritage may immediately terminate this Agreement if Business Associate has breached a material term of the Agreement and cure is not possible.

Termination by Business Associate. If Business Associate knows of a pattern of activity or practice by Covered Entity that constitutes a material breach or violation of Covered Entity's obligations under this Agreement, Business Associate will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful within a period of 30 days, Business Associate will terminate the Agreement, if feasible. See 45 C.F.R. 164.504(e)(1)(iii).

Return or Destruction of Health Information. Upon termination, cancellation, expiration or other conclusion of this Agreement, Business Associate shall return to Heritage or destroy all PHI and EPHI received from Heritage or created or received by Business Associate on behalf of Heritage. This provision shall apply to PHI and EPHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI or EPHI. In the event that Business Associate determines that returning or destroying the PHI or EPHI is infeasible, Business Associate shall provide to Heritage notification of the conditions that make return or destruction infeasible. Upon verification by Heritage that the return or destruction of PHI and/or EPHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and EPHI and limit future uses and disclosure of PHI and EPHI to those purposes that make the return or destruction infeasible for so long as Business Associate maintains such PHI and EPHI.

VI. Miscellaneous

Automatic Amendment. Upon the effective date of any amendment to the regulations promulgated by DHHS with respect to PHI, this Agreement shall automatically amend so that the obligations imposed by Business Associate as a Business Associate remain in compliance with such regulations.

Indemnity. Business Associate agrees to indemnify and hold Heritage harmless against any and all claims, suits, damages, losses, fines, costs, attorneys' fees, and expenses, which Heritage may suffer, incur, or payout by reason of Business Associate's breach of this Agreement, the HIPAA privacy regulations, or applicable HITECH Act provisions with respect to PHI and EPHI of Heritage' s clients.

IN WITNESS WHEREOF, Heritage Area Agency on Aging and the Business Associate have by duly authorized representative entered into the Agreement.

HERITAGE AREA AGENCY ON AGING

By: _____
Signature
Kellie Elliott-Kapparos or Jill Sindt
Co-Directors
Date: _____

BUSINESS ASSOCIATE

By: _____
Signature

_____
Printed Name

_____
Title

_____
Agency Name

_____
Date

Policy 16
Breach of Unsecured PHI

Policy:
It is the policy of Heritage that all employees will access, use and disclose PHI only as permitted under HIPAA, and that all employees shall be vigilant with respect to guarding PHI. However, in the event that a potential breach of unsecured PHI occurs, the following policies and procedures shall be followed.

Procedure:

A. Step 1 – DISCOVERY

i. A breach of PHI will be deemed "discovered" as of the first day Heritage knows of the breach or, by exercising reasonable diligence, would or should have known about the breach.

ii. If a potential breach is discovered, it is very time sensitive and must be immediately reported to the Privacy Officer.

Examples of Breaches of Unsecured Protected Health Information

- Stolen lost laptop containing unsecured protected health information.
- Papers containing protected health information found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding).
- Workforce members accessing electronic health records for information on friends or family members out of curiosity/without a business-related purpose.
- Misfiled consumer information in another consumer's medical records which is brought to the organization's attention by the patient.
- Medical record copies in response to a payer's request lost in mailing process and never received.
- Misdirected fax of patient records to a local grocery store instead of the requesting provider's fax.
- Briefcase containing patient medical record documents stolen from car.
- PDA with patient-identifying information lost.
- Intentional and non-work related access by staff member of neighbor's information.

B. Step 2 – INTERNAL REPORTING

i. If you believe that a potential breach of PHI has occurred, you must immediately notify the Privacy Officer.

ii. Please provide all of the information you have available to you regarding the potential breach, including names, dates, the nature of the PHI potentially breached, the manner of the disclosure (fax, email, mail, verbal), all employees involved, the recipient, all other persons with knowledge, and any associated written or electronic documentation that may exist.

iii. Notification and associated documentation may itself contain PHI and should only be given to the Privacy Officer.

iv. Please do not discuss the potential breach with anyone else, and do not attempt to conduct an investigation. These tasks will be performed by the Privacy Officer.

C. Step 3 – INVESTIGATION

i. Upon receipt of notification of a potential breach the Privacy Officer, or his/her designee, shall promptly conduct an investigation.

ii. The investigation shall include interviewing employees involved, collecting written documentation, and completing all appropriate documentation.

iii. The Privacy Officer shall retain all documentation related to potential breach investigations for a minimum of six years.

D. Step 4 - RISK ASSESSMENT AND RECOMMENDATION TO THE EXECUTIVE DIRECTOR

After the investigation is complete, the Privacy Officer will perform a Risk Assessment using the attached form. The purpose of the Risk Assessment is to determine if a use or disclosure of PHI constitutes a breach and requires further notification. The Privacy Officer shall appropriately document the Risk Assessment and make a recommendation to the Executive Director regarding whether notification to the affected individual(s), HHS and/or the media (as the circumstances dictate) of the potential breach would be required or prudent.

Any acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rules is presumed to be a breach unless the Privacy Officer demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

E. Step 5 – FINAL DETERMINATION BY THE PRIVACY COMMITTEE

The Privacy Officer/Executive Director shall have final authority to determine whether a breach of unsecured PHI occurred and what, if any, further action is warranted.

Breach Notification Risk Assessment Tool[2]

Incident/Name	**Date of event**
Number of individuals affected	
Point of Contact	**Phone #**
Brief Summary/Findings	**Final Decision**

Source of Incident: Who was responsible for the inappropriate access, use or disclosure (incident)? *Circle your answer…* If Business Associate is the source of the incident, enter the date the Business Associate made us aware of incident.	Internal to our organization or Business Associate **Date:**
Are we the Business Associate? *Circle your answer…* If we are the Business Associate, enter the date we notified the other Covered Entity of the incident Enter the date that our organization became aware of the incident	**Yes / No** **Date:** **Date:**

Section 164.404(a)(2) further provides that a covered entity is 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 agent of the covered entity (determined in accordance with the federal common law of agency).

Additional information considered in your determination:

Analysis
Mitigation

[2] Copyright (c) 2009 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works.

Section 1	
1. Is there a HIPAA Security/Privacy Rule violation? ***If No, then STOP here. No breach has occurred that requires notification.*** ***If Yes, then proceed to next question.***	Y/N
2. Was data secured or properly destroyed in compliance with the requirements in the Breach Notification Rule? ***If Yes, then STOP here. No breach has occurred that requires notification.*** ***If No, then proceed to next question.***	Y/N
3. Does this incident qualify as one of the following exceptions? ***If Yes, then STOP here. No breach has occurred that requires notification.*** ***If No, then proceed to next section to work through the rest of the assessment to determine if the breach poses a significant risk to the financial, reputational, or other harm to the individual to the extent that it would require notification.***	Y/N
Note: *The Examples below were taken directly from the Interim Final Rule. See* ***Addendum B*** *for complete regulation text of each exception listed below.*	
a. Good faith, unintentional acquisition, access or use of PHI by employee/workforce *Example- A billing employee receives and opens an e-mail containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then deletes it.*	
b. Inadvertent disclosure to another authorized person within the entity or OHCA *Example- a physician who has authority to use or disclose protected health information at a hospital by virtue of participating in an organized health care arrangement with the hospital is similarly situated to a nurse or billing employee at the hospital.*	
c. Recipient could not reasonably have retained the data *Example, a covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. In these circumstances, the covered entity can conclude that the improper addressees could not reasonably have retained the information.*	

If you did not hit a STOP above in Section 1, then work through the rest of the assessment to determine if the *breach poses a significant risk to the financial, reputational, or other harm to the individual to the extent that it would require notification.*

Go to Section 2

Circle **all that apply** in each subsection:

Section 2		
Variable	**Options**	**Score**
I. Method of Disclosure	• Verbal	1
	• Paper	2
	• Electronic	3
II. Recipient(s)	• Your Business Associate • Another Covered Entity • Internal Workforce	1
	• Wrong Payor (not the patient's) • Unauthorized family member • Non-covered entity	2
	• Media • Unknown/Lost/Stolen • Member of the general public	3
III. Circumstances of release	• Unintentional disclosure of PHI	1
	• Intentional use/access w/o auth • Intentional disclosure w/o auth • Theft – Device targeted • Lost	2
	• Using false pretense to obtain or disclose • Obtained for personal gain/malicious harm • Hack • Theft – data targeted	3
IV. Disposition (What happened to the information after the initial disclosure)	• Information returned complete • Information properly destroyed and attested to	1
	• Information properly destroyed (unattested) • Electronically Deleted (unsure of backup status)	2
	• Sent to the Media • Unable to retrieve • Unsure of disposition or location • High (suspicion of pending re-disclosure) • Extremely High (PHI already re-disclosed)	3
V. Additional Controls	• Data Wiped • Information/Device Encrypted, but does not meet compliance with NIST Standards • Information Destroyed, but does not meet compliance with NIST Standards	1
	• Password protected – password not compromised	2
	• Password protected – password was compromised • No Controls • Other _____	3
Section 2 - Total	***Add highest score from each subsection above and enter here…***	

Circle **ALL** that apply:

Section 3

Below are general guidelines for ranking levels of risks for different types of information breached. ***The circumstances surrounding each breach may impact how you will rank the risk level for the data breached.*** *For example, if a file of known abuse victims is breached that includes the victims' addresses, then you will probably want to rank the breach of this data as a high probability of causing harm to the person(s) impacted by the breach. However, under other circumstances just the release of an address may be considered a low risk of harm to the person(s) impacted by the breach.*

Variable	Options – Type of Information Involved	Score
VI. Type of Info. Breach	**Low Probability that PHI has been compromised** • Limited Data Set *(evaluate possibility of re-identification if ZIP Code and/or DOB included)* • Only identifiers are breached that are not defined under IA Identity Theft Statute and no other health information is breached: name, address, city, state, telephone number, fax number, e-mail address, admission/discharge dates, service dates, date of death	1
	Medium Probability that PHI has been compromised • Non-Sensitive Protected Health Information which may include information about treatment, [3]diagnosis, service, medication, etc… *(Evaluate closely the possibility of the information causing harm to the person(s) impacted by the breach, because the information breached may not typically fall under our definition of sensitive information, but looking at the circumstances it may still cause harm to the individual.)*	2
	Highest Probability that PHI has been compromised • Protected Health Information of a sensitive nature. Information defined by the Iowa Identity Theft Statute which includes the following: o Name o Address o Date of birth o Telephone number o Driver's license number o Nonoperator's identification card number o Social security number o Student identification number, o Military identification number o Alien identification or citizenship status number o Employer identification number o Signature o Electronic mail signature o Electronic identifier or screen name o Biometric identifier o Genetic identification information o Access device o Logo o Symbol o Trademark o Place of employment o Employee identification number o Parent's legal surname prior to marriage o Demand deposit account number	3

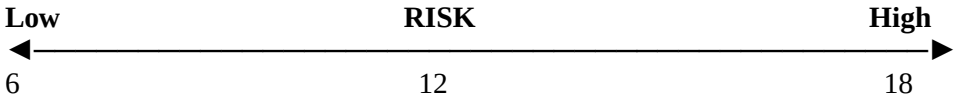
[3] *Further, in the regulations at §164.404(c)(1)(B), the term "diagnosis" is included in the parenthetical listing of examples of types of protected health information to make clear that, where appropriate, a covered entity may need to indicate in the notification to the individual whether and what types of treatment information were involved in a breach.*

	○ Savings or checking account number ○ Credit card number of a person • Sensitive Protected Health Information may also include information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health.	
Section 3 - Total	***Enter highest score selected above in Section 3 here…***	

SCORING

The scoring is meant to serve as a guide in your decision making and not designed to make the decision for you. There are a variety of factors and mitigations that may be involved in your incident that this tool cannot foresee or predict. An attempt was made to develop this is a way that would help you in documenting your actions, consider factors and circumstances and then aid in your final decision of making a breach notification or not making a breach notification.

The range of scoring is 6 -18. A low score of 6 does not necessarily mean you should not take any action but a high score of or near 18 could indicate either a need to notify or a need to take further actions.



Total Risk Score *(Section 2 + Section 3)*	

After completing the assessment and scoring your responses do you feel that the acquisition, access, use or disclosure of PHI poses more than a low probability that the PHI has been compromised?

If **yes**, contact legal counsel immediately to ensure compliance with the notification requirements.

Note that in all cases, if you are unsure, the presumption should be in favor of finding that a breach occurred and notification is required.

Addendum "B" HIPAA Omnibus Rule Definitions (45 C.F.R. 164.402)

"Breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) **Breach excludes**:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a 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 subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further, used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a 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 information.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.