FRESHWATER EDUCATION DISTRICT
ORGANIZED HEALTHCARE ARRANGEMENT
HIPAA PRIVACY POLICIES & PROCEDURES AND ADMINISTRATIVE FORMS
TABLE OF CONTENTS

a. Request for Confidential Communications (Administrative Form)
b. Restricted Uses and Confidential Communication Request Tracking Log (Administrative Form)

12. Privacy Complaint Procedure (Policy & Procedure)
    a. Privacy Complaint Form (Administrative Form)
    b. Response to Privacy Complaint (Administrative Form)
    c. Complaint Tracking Log (Administrative Form)
13. Authorization for Use or Disclosure of PHI (Policy & Procedure) (updated for HITECH)
    a. Authorization for Use or Disclosure (Administrative Form)
14. Revocation of an Authorization (Policy & Procedure)
    a. Revocation by Subject of Protected Health Information (Administrative Form)
15. Business Associates and Business Associate Agreements (Policy & Procedure) (updated for security)
16. Retention of PHI Documentation (Policy & Procedure) (updated for security)
17. HIPAA Privacy and Security Training Program (Policy & Procedure) (updated for security)
    a. Acknowledgment of Training Attendance (Administrative Form)
18. Personal Representative (Policy & Procedure)
    a. Designation of Personal Representative (Administrative Form)
19. Coordination with Other Laws (Policy & Procedure) (updated for security)
20. Disclosures to Plan Sponsor (Policy & Procedure) (updated for security)
21. Duty to Mitigate (Policy & Procedure) (updated for security)
22. Discipline Policy (Policy & Procedure) (updated for security)
23. Administrative, Physical, and Technical Safeguards (Policy & Procedure) (updated for security)
    23-1. Computer Terminals/Workstations (Policy & Procedure) (updated for security)
    23-2. Electronic Mail (E-mail) and Internet System (Policy & Procedure) (updated for security)
    23-3. Facsimile Machines (Policy & Procedure)
    23-4. Copy Machines (Policy & Procedure)
    23-5. Mail – Internal and External (Policy & Procedure)
    23-6. Storage of Documents (Policy & Procedure)
24. Breach Notification (Policy & Procedure) (updated for HITECH)
25. Telecommuting (Policy & Procedure)

HIPAA Privacy Policies and Procedures Overview

[HIPAA Privacy and Security]

Policy Statement

HIPAA requires covered entities to have policies and procedures reflecting HIPAA's privacy and security mandates. The Health Plan, as a covered entity, has developed administrative policies and procedures reflecting the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security regulations.

Policy Interpretation and Implementation

HIPAA Policies and Procedures

1. HIPAA requires covered entities to have policies and procedures to ensure compliance with HIPAA's regulations. A health plan is a "covered entity" under HIPAA. Consequently, the Health Plan is responsible for the research, development, implementation, monitoring and maintenance of the Health Plan's HIPAA privacy and security policies and procedures regarding protected health information (PHI) and electronic protected health information (ePHI).

Health Plan

2. HIPAA defines a "health plan" as an individual or group health plan that provides or pays the cost of medical care, including, but not limited to, employee welfare benefit plans covered by ERISA, health insurers, HMOs, group health plans, and many public benefit programs (Medicaid, Medicare, etc.).

Definition of Protected Health Information (PHI)

3. Protected Health Information (PHI) means individually identifiable information relating to:
   a. The past, present or future physical or mental health or condition of an individual;
   b. The provision of health care to an individual;
   c. The past, present or future payment for health care provided to an individual.

Definition of Electronic Protected Health Information (ePHI)

4. Electronic Protected Health Information (ePHI) means PHI maintained or transmitted in electronic media, including, but not limited to, electronic storage media (i.e., hard drives, digital memory medium) and transmission media used to exchange information in electronic storage media (i.e., internet, extranet, and other networks). PHI transmitted via facsimile and telephone is not considered to be transmissions via electronic media.

Revisions to HIPAA Policies and Procedures

5. The Health Plan's HIPAA policies and procedures may be revised at any time, in order to comply or enhance compliance with HIPAA.

Policy Inquiries

6. Inquiries relative to HIPAA policies and procedures should be directed to the HIPAA Privacy Officer or the HIPAA Security Officer.

Specific Policies and Procedures

7. The Health Plan's specific policies and procedures have been created in order to satisfy HIPAA's requirements.

Organized Health Care Arrangement (OHCA)

8. HIPAA recognizes Organized Health Care Arrangements (OHCAs). An OHCA can exist when an employer sponsors more than one health plan that is a covered entity. Being part of an OHCA allows the covered entities to satisfy the HIPAA privacy and security requirements together, as if they are a single covered entity. The following covered entities are designated as an OHCA:

    - Freshwater Education District Group Medical Plan
    - Freshwater Education District Health Reimbursement Arrangement
    - Freshwater Education District Employee Assistance Plan
    - Freshwater Education District Health Care Expense Reimbursement Plan

    For purposes of these HIPAA policies and procedures, "Health Plan" means the OHCA designated above and "Plan Sponsor" means Freshwater Education District.

Other Laws

9. In addition to HIPAA, covered entities may be subject to other laws that address the privacy and/or security of health information that constitutes PHI. HIPAA establishes a floor – the minimum requirements with which a covered entity must comply. To the extent the requirements of any other law provide more protection to the subject of the health information, those requirements will apply.

Third Party Service Providers

10. Nothing precludes the Health Plan from contracting with a third party service for assistance in complying with the Health Plan's HIPAA policies and procedures.

Record Retention

11. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

12. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

13. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except

holidays at 218-894-2439 x1035.

Violations 14. Violations of this policy will be subject to discipline.

Effective Date 15. July 1, 2014.

References:
45 C.F.R. § 164.530, 45 C.F.R. § 164.306

HIPAA Privacy Officer and Security Officer

[HIPAA Privacy and Security]

Policy Statement

A HIPAA Privacy Officer and a HIPAA Security Officer have been designated by this Health Plan to be responsible for the development and implementation of this Health Plan's HIPAA policies and procedures.

Policy Interpretation and Implementation

Appointment of HIPAA Privacy Officer

1. The Health Plan has appointed the Business Manager of the Plan Sponsor as the Health Plan's HIPAA Privacy Officer.

Appointment of HIPAA Security Officer

2. The Health Plan has appointed the Payroll Clerk of the Plan Sponsor as the Health Plan's HIPAA Security Officer.

HIPAA Privacy Officer's Responsibilities

3. The HIPAA Privacy Officer's responsibilities include:
   a. Assisting management in the development, implementation, and updating of the Health Plan's HIPAA policies and procedures;
   b. Performing periodic privacy risk assessments;
   c. Assisting management in implementing procedures to restrict access to protected health information (PHI) by authorized users;
   d. Receiving complaints concerning the Health Plan's HIPAA policies and procedures;
   e. Receiving complaints concerning the Health Plan's compliance with its established policies and procedures;
   f. Maintaining a complaint tracking log;
   g. Assisting in obtaining use and disclosure of PHI authorizations;
   h. Assisting in the development of training materials and training to ensure that relevant staff are well trained in matters relating to the use and disclosure of protected health information (PHI);
   i. Providing staff, individuals, business associates, and government agencies with information regarding the Health Plan's HIPAA policies and procedures; and
   j. Working with the Health Plan's legal counsel on matters relative to HIPAA.

HIPAA Security Officer's Responsibilities

4. The HIPAA Security Officer's responsibilities include:
   a. Assisting management in the development, implementation, and updating of the Health Plan's HIPAA policies and procedures;
   b. Performing periodic security risk assessments;
   c. Development of security procedures and guidelines for the protection of the Health Plan's information systems;
   d. Assisting management in the assigning of passwords and user identification codes for access to electronic

protected health information (ePHI) by authorized users;

e. Assisting in the development of training materials and training to ensure that relevant staff are well trained in matters relating to the protection and safeguarding of ePHI;

f. Providing staff, individuals, business associates, and government agencies with information regarding the Health Plan's HIPAA policies and procedures; and

g. Working with the Health Plan's legal counsel on matters relative to HIPAA.

Delegation

5. The HIPAA Privacy Officer and Security Officer may delegate certain job functions to be performed by other individuals; however, the ultimate responsibility for compliance with HIPAA remains with the HIPAA Privacy Officer and Security Officer.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

8. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. July 1, 2014.

References:

45 C.F.R. § 164.530(a), 45 C.F.R. § 164.308(a)(2)

Notice of Privacy Practices

Policy Statement

Each individual that is the subject of Protected Health Information (PHI), including electronic protected health information (ePHI), must receive a Notice of Privacy Practices (NPP) describing (1) the uses and disclosures of his/her PHI that may be made by or on behalf of the Health Plan, (2) the individual's rights, and (3) the Health Plan's legal duties with respect to the individual's PHI.

Policy Interpretation and Implementation

Issuance of NPP

1. Individuals who are covered under the Health Plan will be provided with a copy of the Health Plan's NPP.

Content of NPP

2. NPPs must be prepared in easy to read language and contain, as a minimum, the following elements:
    a. A statement indicating how medical information about the individual may be used and disclosed and how the individual can obtain access to such information;
    b. A description, including at least one example, of the types of uses and disclosures that the Health Plan is permitted to make for purposes of treatment, payment and healthcare operations, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required;
    c. A description of each of the other purposes for which the Health Plan is permitted or required to use or disclose PHI without the individual's consent or authorization, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required;
    d. A statement that other uses or disclosures will be made only with the individual's written authorization, and that the authorization may be revoked in accordance with the policy on authorization;
    e. A statement of the individual's rights with respect to his/her PHI, and a brief description of how the individual may exercise those rights, including:
        i. The right to request restrictions on certain uses/disclosures of PHI, and the fact that the Health Plan may not have to agree to such restrictions;
        ii. The right to receive confidential communications of PHI;
        iii. The right to inspect and copy PHI;
        iv. The right to amend PHI;

v. The right to receive an accounting of disclosures of PHI; and

vi. The right to receive a paper copy of the privacy notice.

f. A statement of the Health Plan's duties with respect to PHI, including statements:

i. That the Health Plan is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices;

ii. That the Health Plan is required to abide by the terms of its current effective privacy notice; and

iii. That the Health Plan reserves the right to change the terms of the notice and make a new notice provision effective for all PHI maintained, along with a description of how the Health Plan will provide individuals with the revised notice.

g. A statement that individuals may complain to the Health Plan and to the Secretary of the U.S. Department of Health and Human Services about privacy rights violations, including a brief statement about how a complaint may be filed and an assurance that the individual will not be retaliated against for filing a complaint;

h. The name, or title, and telephone number of the Health Plan's HIPAA Privacy Officer to contact for further information;

i. The name, telephone number and address of the person designated by the Health Plan to receive complaints regarding the Health Plan's privacy practices; and

j. The effective date of the NPP, which may not be earlier than the date printed or published.

Modification of NPP

3. The Health Plan will amend the NPP in the following circumstances:

a. HIPAA, or the regulations thereunder, are amended to require additional or different content in the NPP; and

b. Upon a change to the Health Plan's policies or procedures that impacts the content of the NPP.

Distribution of NPP

4. The Health Plan will distribute the NPPs at the times specified below:
   a. On the Health Plan's initial compliance date;
   b. At the time of enrollment in the Health Plan for new enrollees; and
   c. Within sixty (60) days of a material revision of the NPP to individuals covered by the Health Plan.
5. The NPP will be distributed no less frequently than once every three (3) years.
6. The NPP will be delivered by first class U.S. Mail to the address of record on file with the Health Plan. The NPP will be addressed to the individual, spouse and all dependents covered by the Health Plan.

Posting of NPP

7. A copy of the NPP will be posted on the web page, if one exists, of the employer sponsoring the Health Plan. The HIPAA Privacy Officer is responsible for prompt distribution of changes to the privacy notice.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

9. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

10. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Effective Date

11. July 1, 2014.

References:
45 C.F.R. § 164.520

FRESHWATER EDUCATION DISTRICT
ORGANIZED HEALTH CARE ARRANGEMENT
NOTICE OF PRIVACY PRACTICES

Effective _____

This Notice Describes How Medical Information About You May Be Used and Disclosed and How You Can Get Access To This Information. Please Review It Carefully.

If you have any questions about this notice, please contact the **Privacy Officer**:

<<title>>
<<address>>
<<phone>>
<<fax>>
<<e-mail address>>

Who Will Follow This Notice

This notice describes the medical information practices of the <<name of company>> organized health care arrangement (OHCA) and third parties that assist in the administration of the OHCA Plans.

For purposes of HIPAA and this notice, the OHCA includes the following:

- <<list all plans affected by HIPAA>>
-
-
-
-

Our Pledge Regarding Medical Information

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. This notice applies to all of the medical records maintained by an OHCA Plan. Your personal doctor or health care provider may have different policies or notices regarding the doctor's use and disclosure of your medical information created in the doctor's office or clinic.

This notice tells you about the ways in which we may use and disclose medical information about you. It also describes our obligations and your rights regarding the use and disclosure of medical information.

We are required by law to:

- make sure that medical information that identifies you is kept private;
- give you this notice of our legal duties and privacy practices with respect to medical information about you; and
- follow the terms of the notice that are currently in effect.

How We May Use and Disclose Medical Information About You

The following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures, we will explain what we mean and present some examples. These

examples are not exhaustive. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

Please note: In most instances, how information is used and disclosed has not changed. The descriptions reflect how the Health Plans that make up the OHCA have traditionally operated.

For Treatment (as described in applicable regulations). We may use or disclose medical information about you to facilitate medical treatment or services by providers. We may disclose medical information about you to providers, including doctors, nurses, technicians, medical students, or other hospital personnel who are involved in taking care of you.

For Payment (as described in applicable regulations). We may use and disclose medical information about you to determine eligibility for benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under an OHCA Plan, or to coordinate OHCA Plan coverage. For example, we may tell your health care provider about your medical history to determine whether a particular treatment is experimental, investigational, or medically necessary or to determine whether the OHCA Plan covers the treatment. We may also share medical information with a utilization review or pre-certification service provider. Likewise, we may share medical information with another entity to assist with the adjudication (legal actions) or subrogation (third party reimbursements) of health claims or to another health plan to coordinate benefit payments.

For Health Care Operations (as described in applicable regulations). We may use and disclose medical information about you for other OHCA Plan operations. These uses and disclosures are necessary to run the OHCA Plan. For example, we may use medical information in connection with: conducting quality assessment and improvement activities; underwriting, premium rating, and other activities relating to OHCA Plan coverage; submitting claims for stop-loss (or excess loss) coverage; conducting or arranging for medical review, legal services, audit services, and fraud and abuse detection programs; business planning and development such as cost management; and business management and general OHCA Plan administrative activities. We will not, however, use genetic information about you for underwriting purposes.

To Business Associates. We may contract with individuals or entities known as Business Associates to perform various functions on our behalf or to provide certain types of services. In order to perform these functions or provide these services, Business Associates will receive, create, maintain, use and/or disclose your protected health information, but only after they agree in writing with us to implement appropriate safeguards regarding your protected health information. For example, we may disclose your protected health information to a Business Associate to administer claims or to provide support services, such as utilization management, pharmacy benefit management or subrogation, but only after the Business Associate enters into a Business Associate contract with us.

As Required By Law. We will disclose medical information about you when required to do so by federal, state or local law. For example, we may disclose medical information when required by a court order or subpoena.

To Avert a Serious Threat to Health or Safety. An OHCA may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. However disclosure would be limited to someone able to help prevent the threat.

Special Situations

Disclosure to Health Plan Sponsor. Information may be disclosed to another health plan for purposes of facilitating claims payments under that plan. In addition, medical information may be disclosed to <<name of company>> personnel solely for administering benefits under the OHCA Plan.

Organ and Tissue Donation. If you are an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

Military and Veterans. If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

Workers' Compensation. We may release medical information about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Public Health Risks. We may disclose medical information about you for public health activities. These activities generally include the following:

- to prevent or control disease, injury or disability;
- to report births and deaths;
- to report reactions to medications or problems with products;
- to notify people of recalls of products they may be using;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- to notify the appropriate government authority if we believe an individual has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

Health Oversight Activities. We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Law Enforcement. We may release medical information if asked to do so by a law enforcement official:

- in response to a court order, subpoena, warrant, summons or similar process;
- to identify or locate a suspect, fugitive, material witness, or missing person;
- about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
- about a death we believe may be the result of criminal conduct; and
- in emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

Coroners and Medical Examiners. We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death.

National Security and Intelligence Activities. We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

Research. We may disclose your protected health information to researchers when:

(1) the individual identifiers have been removed; or

(2) when an institutional review board or privacy board has reviewed the research proposal and established protocols to ensure the privacy of the requested information, and approves the research.

Required Disclosures

Government Audits. We are required to disclose your protected health information to the Secretary of the United States Department of Health and Human Services when the Secretary is investigating or determining our compliance with the HIPAA privacy rule.

Disclosures to You. When you request, we are required to disclose to you the portion of your protected health information that contains medical records, billing records, and any other records used to make decisions regarding your health care benefits. We are also required, when requested, to provide you with an accounting of most disclosures of your protected health information if the disclosure was for reasons other than for payment, treatment, or health care operations, and if the protected health information was not disclosed pursuant to your individual authorization.

Other Disclosures

Personal Representatives. We will disclose your protected health information to individuals authorized by you, or to an individual designated as your personal representative, attorney-in-fact, etc., so long as you provide us with a written notice/authorization and any supporting documents (i.e., power of attorney). Note: Under the HIPAA privacy rule, we do not have to disclose information to a personal representative if we have a reasonable belief that:

(1) you have been, or may be, subjected to domestic violence, abuse or neglect by such person; or

(2) treating such person as your personal representative could endanger you; and

(3) in the exercise of professional judgment, it is not in your best interest to treat the person as your personal representative.

Spouses and Other Family Members. With only limited exceptions, we will send all mail to the employee. This includes mail relating to the employee's spouse and other family members who are

covered under the OHCA Plan, and includes mail with information on the use of OHCA Plan benefits by the employee's spouse and other family members and information on the denial of any OHCA Plan benefits to the employee's spouse and other family members. If a person covered under the OHCA Plan has requested Restrictions or Confidential Communications (see below under "Your Rights"), and if we have agreed to the request, we will send mail as provided by the request for Restrictions or Confidential Communications.

Authorizations. Other uses or disclosures of your protected health information not described above will only be made with your written authorization. For example, in general and subject to specific conditions, we will not use or disclose your psychiatric notes, use or disclose your protected health information for marketing, or sell your protected health information without your written authorization. You may revoke written authorization at any time, so long as the revocation is in writing. Once we receive your written revocation, it will only be effective for future uses and disclosures. It will not be effective for any information that may have been used or disclosed in reliance upon the written authorization and prior to receiving your written revocation.

Your Rights Regarding Medical Information About You

You have the following rights regarding medical information we maintain about you:

Right to Inspect and Copy. You have the right to inspect and copy medical information that may be used to make decisions about your OHCA Plan benefits. If the information you request is maintained electronically, and you request an electronic copy, we will provide a copy in the electronic form and format you request if the information can be readily produced in that form and format. If the information cannot be readily produced in that form and format, we will work with you to agree on an alternative electronic form and format. If we cannot agree on an electronic form and format, we will provide you with a paper copy.

To inspect and copy the medical information that may be used to make decisions about you, you must submit your request in writing to the Privacy Officer. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies associated with your request.

We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed.

Right to Amend. If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the OHCA Plan.

To request an amendment, your request must be made in writing and submitted to the Privacy Officer. In addition, you must provide a reason that supports your request.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

- is not part of the medical information kept by or for the OHCA Plan;
- was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the information which you would be permitted to inspect and copy; or new is accurate and complete.

Right to an Accounting of Disclosures. You have the right to request an "accounting of disclosures" where such disclosure was made for any purpose other than treatment, payment, or health care

operations. The accounting will not include (1) disclosures for purposes of treatment, payment, or health care operations; (2) disclosures made to you; (3) disclosures made pursuant to your authorization; (4) disclosures made to friends or family in your presence or because of an emergency; (5) disclosures for national security purposes; and (6) disclosures incidental to otherwise permissible disclosures.

To request this list of accounting of disclosures, you must submit your request in writing to Privacy Officer. Your request must state a time period which may not be longer than six years from the date of the request. Your request should indicate in what form you want the list (for example, paper or electronic). The first list you request within a 12 month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

Right to Request Restrictions. You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had.

To request restrictions, you must make your request in writing to the Privacy Officer. Except as provided in the next paragraph, we are not required to agree to your request. However, if we do agree to the request, we will honor the restriction until you revoke it or we notify you.

We will comply with any restriction request if (1) except as otherwise required by law, the disclosure is to the health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full.

In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse.

Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. To request confidential communications, you must make your request in writing to the Privacy Officer. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

Right to Be Notified of a Breach. You have the right to be notified in the event that we (or a Business Associate) discover a breach of unsecured protected health information.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice.

You may obtain a copy of this notice at our website, <<website address>>.
To obtain a paper copy of this notice, contact the Privacy Officer.

Changes to This Notice

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the

future. We will post a copy of the revised or changed notice on our website and will mail a copy of it to you. The notice will contain an effective date on the first page.

Complaints

If you believe your privacy rights have been violated, you may file a complaint with the OHCA Plan or with the Secretary of the Department of Health and Human Services. To file a complaint with the OHCA Plan, contact the Privacy Officer. All complaints must be submitted in writing. To file a complaint with the Department of Health and Human Services Office of Civil Rights, send a letter to 200 Independence Avenue S.W., Washington D.C. 20201, call 1-877-696-6775, or visit www.hhs.gov/ocr/privacy/hipaa/compaints/.

You will not be penalized for filing a complaint.

Other Uses of Medical Information

Other uses and disclosures of medical information not covered by this notice or the other applicable laws will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

Use or Disclosure of PHI

[HIPAA Privacy and Security]

Policy Statement

In order for the Health Plan to use or disclose (including obtaining) protected health information (PHI), including electronic protected health information (ePHI), the use or disclosure must either (1) fall under the enumerated uses and disclosures allowed without an individual authorization, or (2) the Health Plan must obtain an individual authorization.

Policy Interpretation and Implementation

Definition of Protected Health Information (PHI)

1. Protected Health Information (PHI) means individually identifiable information relating to:
    a. The past, present or future physical or mental health or condition of an individual;
    b. The provision of health care to an individual;
    c. The past, present or future payment for health care provided to an individual.

Definition of Electronic Protected Health Information (ePHI)

2. Electronic Protected Health Information (ePHI) means PHI maintained or transmitted in electronic media, including, but not limited to, electronic storage media (i.e., hard drives, digital memory medium) and transmission media used to exchange information in electronic storage media (i.e., internet, extranet, and other networks). PHI transmitted via facsimile and telephone is not considered to be transmissions via electronic media.

Use and Disclosure not Requiring an Individual Authorization

3. PHI may be used or disclosed without an individual authorization only for treatment, payment, or health care operations (TPO). These purposes include:
    a. The Health Plan may use or disclose PHI for its own TPO;
    b. The Health Plan may disclose PHI to another covered entity for the payment activities of that entity;
    c. The Health Plan may disclose PHI to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the PHI, the PHI pertains to such relationship, and the disclosure is:
        i. For health care operations regarding conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, and related functions that do not

include treatment, reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, credentialing activities; or

ii. For the purpose of health care fraud and abuse detection or compliance;

d. If the Health Plan participates in an organized health care arrangement (OHCA), it may disclose PHI about an individual to another covered entity that participates in the OHCA for any health care operations activities of the OHCA.

Nothing in paragraph 2 prevents the Health Plan from obtaining an individual authorization for use and disclosure of PHI for TPO purposes.

Definition of Treatment, Payment and Health Care Operations (TPO)

4. Treatment, Payment and Health Care Operations (TPO) includes all of the following:

   a. Treatment means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual or referral of an individual to another provider for health care.

   b. Payment means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.

   c. Health Care Operations includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services, and auditing functions, business planning and development, and general business and administrative activities.

Note: Notwithstanding the foregoing, the Health Plan shall not use genetic information for underwriting purposes.

Disclosure to Family Members and Others

5. The Health Plan may disclose to a family member, other relative, or a close personal friend of the individual who is the subject of the PHI, or any other person identify by the individual, if such person is involved in the individual's care or payment related to the individual's care, the PHI directly relevant to such person's involvement. To the extent allowed by HIPAA, such disclosures may be made with respect to PHI regarding a deceased individual to family members or others who were involved in the decedent's care or payment related to the decedent's care. If the individual is available prior to a disclosure governed by this provision, the Health Plan will not disclose the PHI unless it has:
   a. Obtained the individual's agreement to the disclosure;
   b. Provided the individual an opportunity to object to the disclosure, and the individual has not objected; or
   c. Reasonably infers from the circumstances, based upon the exercise of professional judgment, that the individual does not object to the disclosure.

Use and Disclosure for Public Policy Reasons

6. PHI may be used or disclosed without an individual authorization as required by law and for other public policy reasons when specific requirements are met. The situations in which PHI may be disclosed for public policy reasons include, but are not limited to, situations involving:
   a. serious threats to health or safety;
   b. disclosures to health plan sponsor;
   c. organ and tissue donation;
   d. military and veterans;
   e. workers' compensation;
   f. public health risks;
   g. health oversight activities;
   h. lawsuits and disputes;
   i. law enforcement;
   j. coroners, medical examiners and funeral directors;
   k. national security and intelligence activities; and
   l. inmates.

Use and Disclosure Requiring an Individual Authorization

7. An individual authorization is required for any use or disclosure of PHI that is not specifically allowed by the HIPAA privacy regulations (without the individual authorization). These uses and disclosures include, but are not limited to:
   a. Use or disclosure of psychotherapy notes;
   b. Exchange of PHI for direct or indirect remuneration; and
   c. Use or disclosure of PHI for purposes of

"marketing" (as that term is defined in 45 C.F.R. Section 164.501, except if the communication is in the form of:

i. Face-to-face communication made by the Health Plan to an individual; or

ii. A promotional gift of nominal value provided by the Health Plan.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

9. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

10. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

11. Violations of this policy will be subject to discipline.

Effective Date

12. July 1, 2014.

References:

45 C.F.R. §§164.501, 164.506, 164.508, 164.510(b), 164.512

Minimum Necessary Standard

[HIPAA Privacy and Security]

Policy Statement

Whenever practical/feasible, the Health Plan will make reasonable efforts to limit use and disclosure of protected health information (PHI), including electronic protected health information (ePHI), to the minimum necessary to accomplish the appropriate intended purpose.

Policy Interpretation and Implementation

Minimum Necessary Standard

1. When using, disclosing, transmitting, or requesting PHI, including ePHI, the Health Plan shall make reasonable efforts to limit the PHI (including ePHI) used, disclosed, transmitted, or requested to the minimum necessary to accomplish the purpose. Until the issuance of further guidance regarding the minimum necessary standard, the Health Plan will limit the PHI (including ePHI) used, disclosed, transmitted, or requested to the limited data set and such limitation shall satisfy the minimum necessary standard. Notwithstanding the foregoing, the Health Plan reserves the right to use, disclose, transmit, or request the minimum necessary PHI (including ePHI), if the limited data set will not meet the needs of a particular use, disclosure, or request.

   Limited data set means PHI that excludes certain direct identifiers of the individual or of relatives, employers, or household members of the individual, as identified in Section 164.514(e)(2) of the HIPAA regulations.

Access to PHI/ePHI

2. The Health Plan requires relevant staff to have access only to the minimum necessary PHI, including ePHI, required by their job functions.

   It is the responsibility of the HIPAA Privacy Officer and the HIPAA Security Officer to limit the access of relevant staff to only the minimum necessary PHI, including ePHI, required by their job function. The HIPAA Privacy Officer and the HIPAA Security Officer may delegate certain job functions to be performed by other individuals; however, the ultimate responsibility for compliance with HIPAA remains with the HIPAA Privacy Officer and the HIPAA Security Officer.

Where Minimum Necessary Standard Does Not Apply

3. Limiting use, disclosure, transmittal, or request of PHI, including ePHI, to the minimum necessary does NOT apply in the following situations:

   a. Disclosures or requests by a health care provider for treatment;

   b. Uses or disclosures made to the individual or requested and authorized by the individual;

c. Disclosures made to the Secretary of Health and Human Services (HHS) or to the Office of Civil Rights (OCR);

d. Uses or disclosures required by law; and/or

e. Uses or disclosures required for compliance with the Privacy Rule and/or the Security Rule.

Disclosures of PHI/ePHI by Health Plan

4. From time to time, relevant staff of the Health Plan will be asked to disclose PHI, including ePHI, to other covered entities, regulatory agencies, law enforcement authorities and others. Many of these disclosures are permitted or required by law and do not require authorization of the individual. Others may require authorization of the individual whose PHI is to be disclosed. Except for those instances identified previously, the Health Plan will apply the minimum necessary standard to all disclosures.

   Relevant staff of the Health Plan may treat a request for a disclosure as being for the minimum necessary PHI, including ePHI, when the request is:

   - From a public official who states that the disclosure is the minimum necessary;
   - From another covered entity;
   - From a professional who is a member of the Health Plan or is a Business Associate of the Health Plan if he/she states that the information is the minimum necessary needed; and
   - For research purposes when the required documentation is provided.

Requests for PHI/ePHI by Health Plan

5. Relevant staff of the Health Plan must limit requests made by them for PHI, including ePHI, to that which is reasonably necessary to accomplish the purpose of the request.

Entire Medical Record

6. The Health Plan will not use, disclose, transmit, or request an entire medical record unless the entire medical record is specifically justified as reasonably necessary. Unjustified use, disclosure, transmittal, or request of an entire medical record will be considered a violation of this policy. The only exception regarding the entire medical record is when the information is provided to persons involved in the treatment of the individual.

Record Retention

7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

8. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

9. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

10. Violations of this policy will be subject to discipline.

Effective Date

11. July 1, 2014.

References:
45 C.F.R. §§ 164.502(b), 164.514(d)

Individual's Rights to Access & Copy PHI

Policy Statement

Individuals have the right to access and copy their own protected health information (PHI), including electronic protected health information (ePHI), maintained/retained by the Health Plan, including any business associates on behalf of the Health Plan, in their designated record set (DRS).

Policy Interpretation and Implementation

Definition of DRS

1. A group of records maintained by the Health Plan that are:
    a. Medical records and billing records about individuals maintained by or for the Health Plan;
    b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for the Health Plan; or
    c. Used by or for the Health Plan to make decisions about individuals.
2. The term "record" as used above means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the Health Plan.

Individual's Right to Access and Copy PHI

3. An individual generally has a right to access and copy his/her PHI maintained in the DRS.

Written Request

4. Request for inspection and copying of PHI must be submitted to the HIPAA Privacy Officer in writing.

Time Frame for Retrieval of Requested PHI

5. Insofar as practical, the individual should allow at least thirty (30) days for the Health Plan to obtain requested information. Should an extension be necessary, the individual will be notified of such request. In no case may the extension exceed thirty (30) days.

Denial of Access

6. Should the individual be denied access to requested records, a written notice must be provided to the individual indicating such denial and the reason(s) for the denial.

Service Fees

7. The following charge(s) may be assessed for copying services:

    Per Page Fee: $0.10
    Postage Fee: Standard U.S. postage
    Labor Fee: $25 per hour

Exceptions

8. Individuals may be denied access to (1) psychotherapy notes, and (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Denial of Access Without Right of Review

9. Denial of access without a right of review may occur:
    a. Where information was compiled in anticipation of litigation;
    b. Where care was provided under the direction of a correctional institution and provision of access would jeopardize health, safety, or rehabilitation; and
    c. Where information was collected in the course of research that includes treatment of the individual and the individual agreed to a *suspension* of the right of access during the research period.

Denial in Accordance with Other Applicable Law

10. Access may also be denied in accordance with other applicable law.

Denial of Access With Right of Review

11. Denial of access with a right of review may occur:
    a. Where access is determined by a licensed professional to be likely to endanger life or safety of the individual or another person; and
    b. Where access is required by the individual's representative and a licensed professional determines that such access is reasonably likely to cause substantial harm.

Individual's Right to Review by Another Licensed Professional

12. If the basis for denial of access gives the individual a *right to review*, the individual has the right to have the denial reviewed by a licensed professional who did not participate in the original denial decision. Such review will be completed within thirty (30) days of such request. The Health Plan will provide the individual with a notice of the reviewer's decision and will comply with the determination to either provide the requested information or deny access to such requested information.

Time Frame to Act Upon Individual's Request for Access

13. The Health Plan will act upon an individual's request for access to his/her DRS no later than thirty (30) days after receipt of such request, unless the time period is extended as described below:

a. If the information to be accessed is not maintained or accessible on premises, the Health Plan will act upon such request within sixty (60) days of receipt of such request.

b. If the Health Plan is unable to act on the request within the applicable thirty (30) or sixty (60) day period, the Health Plan may extend the time for response by thirty (30) days, provided that the individual is given a written notice of the reason(s) for the delay and the date by which a responsive action will be taken.

Denial of Access Notice

14. The Health Plan will provide a timely, written denial of access to the individual when such denials occur. Denial notices will be written in easy-to-read language and will include, as a minimum, the following information:

    a. The basis for the denial of access;

    b. Any right of review (as applicable);

    c. How to file a complaint with the Health Plan;

    d. The name and telephone number of the person to whom the complaint may be filed; and

    e. The address of the U.S. Secretary of Health and Human Services.

Access to Requested Information

15. To the extent practical, the individual will be given access to any information requested after excluding the information for which the Health Plan has grounds for denying access.

Access to Information Maintained Off Premises

16. Should the information for which access has been requested be maintained off premises or the Health Plan does not maintain/retain such information, but knows where the information is located, the Health Plan will either (a) notify the individual where to direct his/her request for access, or (b) otherwise make arrangements for the individual to access such information. This includes, but is not limited to, information maintained by a business associate on behalf of the Health Plan.

Special Rules Regarding Access to ePHI

17. Notwithstanding anything in this policy to the contrary, the Health Plan will provide an individual (and/or a third party designated by the individual in a signed request) a copy of his/her ePHI maintained in the DRS in the electronic form and format requested by the individual if it is readily producible. If the ePHI is not readily producible in the form and format requested by the individual, the Health Plan will provide a copy of the ePHI in a mutually agreeable, machine readable format. If no electronic format is mutually agreeable, a paper copy will be provided. The Health Plan may charge a reasonable, cost-based fee for providing a copy of the ePHI.

Record Retention

18. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

19. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

20. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

21. Violations of this policy will be subject to discipline.

Effective Date

22. July 1, 2014.

References:

45 C.F.R. § 164.524

REQUEST TO ACCESS OWN PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 6, Individual's Right to Access & Copy PHI.

You have a right to request access to inspect and to receive copies of your protected health information (PHI). Please see the Health Plan's Notice of Privacy Practices **[or contact the Health Plan's Privacy Officer at [xxx-xxx-xxxx]** for more information.

Please submit this form to**:** **[Title]**
[Address]

Your name: _____

Address: _____

Daytime phone number: _____

<u>Please select one</u>:

___ I participate in or am covered under the Health Plan **[name of health plan(s)]**.

___ I am the personal representative of an individual participating in or covered under the Health Plan **[name of health plan(s)]** (*please attach completed Designation of Personal Representative form*).

Access is requested to the following information:

_____
_____
_____

Please provide me with the above information dated between _____and _____.

I prefer to review the information in the following manner (please select one):

___ Mailed copy

___ Electronic copy (if available) (describe form and format): _____

___ View at **[Company]** business offices

___ Other (describe on a separate sheet)

___ I agree to accept a summary of the above requested information and to pay a reasonable charge for the costs incurred by the Health Plan in preparing the summary.

Please Read Carefully and Sign

I understand that the Health Plan will provide the requested inspection or copies if required to do so under applicable law. I also understand that I may be charged for copying and postage in accordance with the Health Plan's Notice of Privacy Practices.

_____ _____

Signature Date

Please note: Applicable law requires us to respond to you within 30 days after receiving your request, unless the information requested is not maintained at our primary business address, in which case we will respond within 60 days. We are entitled, in certain circumstances, to an additional 30 days in which to respond. We will send you written notice if we determine we will need the additional 30 days.

For office use only:

Received by:_____ Date:_____

GRANT OF REQUEST TO ACCESS OWN PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 6, Individual's Right to Access & Copy PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request to access and/or copy your own protected health information (PHI) on **[date]**.

ACCESS

_____ The information to which you requested access will be available as of **[date]** for your review at **[address]**.

_____ There are questions regarding your request for access. Please call us at **[xxx-xxx-xxxx]** so we may discuss the nature and scope of your request.

COPIES

_____ We have enclosed copies of the information you requested. We are permitted under federal law to recover our reasonable copying and postage costs of $____. Please **[promptly]** remit payment **[by check or money order]** to:

[Name]
[Address]

_____ The records you requested are voluminous or are not in a format that is easily copied and mailed. Please call us at **[xxx-xxx-xxxx]** so we may discuss the scope and format of your request, as well as a convenient time and place for you to inspect or obtain a copy of the requested information.

_____ The electronic records you requested are not readily producible in the form and format you requested. Please call us at **[xxx-xxx-xxxx]** so we may discuss the form and format of the requested information.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Sincerely,

[Name]
[Title]

NOTIFICATION OF ADDITIONAL TIME TO RESPOND TO ACCESS TO OWN PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 6, Individual's Rights to Access & Copy PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request to access and/or copy your own protected health information (PHI) on **[date]**. We have been unable to respond due to **[give reason for delay]**. We will respond to your request by **[specific date no more than 30 days from original response due date]**.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Thank you for your patience.

Sincerely,

[Name]
[Title]

DENIAL OF REQUEST TO ACCESS OWN PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 6, Individual's Rights to Access & Copy PHI.

Dear **[participant, beneficiary, or personal representative]**:

We have reviewed your request to access and/or copy your own protected health information (PHI). We are denying your request for the following reasons:

_____ We do not maintain **[part of]** the information you requested. That information is maintained by **[insert description]**. You have no right to appeal this denial.

_____ **[Part of the <or> The]** information you requested is not contained in our designated record sets. This means that we do not use the information you requested to make decisions relating to your health benefits. Accordingly, we are not required to provide it under the federal Privacy Rule. **[We will provide you with access to the part of the information you requested that is in our designated record sets.]** You have no right to appeal this denial.

_____ The Privacy Rule exempts the information you requested from access requests. You have no right to appeal this denial.

_____ We have determined that release of the information you request may result in harm to you or someone else. You may appeal this basis of denial. If you would like to appeal this determination, you may write to us at:

[Name/Department]
[Address]

Complaints. You may submit a complaint about this denial to us. If you choose to do so, please direct your complaint as indicated below. Please note that your complaint is not considered an appeal of our denial.

[Name of complaint contact person/office]
[Address]
[Telephone number]

You may also submit a complaint about this denial of access to the head of the U.S. Department of Health and Human Services. Your complaint must be in writing, either on paper or electronically, and must include the following information: (1) our name, and (2) a description of the acts or omissions that you believe violate our responsibilities under the Privacy Rule. Your complaint must be filed within 180 days from the date of this letter.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Sincerely,

[Name]
[Title]

ACCESS REQUEST TRACKING LOG

Please note: This Administrative Form relates to the Health Plan's Policy Form 6, Individual's Rights to Access & Copy PHI.

Name of Requestor	Date Rec'd	Extension	Granted	Denied[1]	Appeal	Appeal Resolved

[1] Please indicate the following reasons for denial: (a)-not in designated record sets; (b)-"safety" reason; (c)-psychotherapy notes; (d)-requestor not authorized personal representative; (e)-other.

Amendment of the PHI

Policy Statement

An individual may amend his/her protected health information (PHI), including electronic protected health information (ePHI).

Policy Interpretation and Implementation

Amendment of PHI

1. An individual may amend his/her PHI except as outlined below:
   a. The originator of the record is no longer available;
   b. The information the individual wishes to amend was not created by the Health Plan;
   c. The information is not part of the health information record;
   d. The information contained in the record is accurate and complete; and/or
   e. The amended information would not be available as provided by current law.

Written Amendment Request

2. All requests for amendments to PHI must be submitted to the HIPAA Privacy Officer in writing.

Time Frame for Acting Upon a Request for Amendments

3. The Health Plan will act upon the individual's request for an amendment no later than sixty (60) days after receipt of such request. Should the Health Plan be unable to act upon the request within the sixty (60) day period, the individual will be provided with a written notice of the reasons for the delay and the date by which the Health Plan will complete such action. In no case will such extension extend beyond thirty (30) days.

Acceptance of Amendment

4. When the Health Plan accepts the amendment, in whole or in part, the Health Plan will:
   a. Make the requested amendment(s) to the PHI or record that is subject to the amendment(s) or provide a link to the location of such amendment(s);
   b. Inform the individual that the amendment(s) are accepted and have been made;
   c. Notify persons/entities authorized by the individual that such amendments have been made and provide copies of such amendments as requested; and
   d. Notify business associates that such amendments have been made and provide copies of such amendments to business associates as requested.

Denial of Amendment Requests

5. Should the Health Plan **deny** a requested amendment, in whole or in part, the Health Plan will:
   a. Notify the individual in writing of the denial to make an amendment to his/her PHI. Such denial will include the following information:
      i. The reason(s) for the denial;
      ii. Information relative to how the individual may submit a written statement disagreeing with the denial;
      iii. Information relative to how the individual may request that the amendment and the denial become part of the individual's permanent records; and
      iv. Information relative to how the individual may file a complaint with the HIPAA Privacy Officer or to the U.S. Secretary of Health and Human Services.
   b. Include on all notices to the individual the name, title, and telephone number of the contact person or office designated to receive complaints.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

8. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. July 1, 2014.

References:
45 C.F.R. § 164.526

REQUEST FOR AMENDMENT OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of PHI

You have a right to request an amendment of your own protected health information (PHI). Please see the Notice of Privacy Practices **[or contact the Health Plan's Privacy Officer at xxx-xxx-xxxx]** for more information.

Please submit this form to**:** **[Title]**
[Address]

Your name: _____

Address: _____

Daytime phone number: _____

Please select one:

___ I participate in or am covered under the Health Plan **[name of health plan(s)]**.

___ I am the personal representative of an individual participating in or covered under the Health Plan (*please attach completed Designation of Personal Representative form if one is not already on file*).

I would like to request an amendment to the following information: _____
_____
_____
_____

The information should be amended in the following manner: _____
_____
_____
_____

I believe this information should be amended because (required): _____
_____
_____
_____

Please Read Carefully and Sign

I understand that the Health Plan will agree to my requested amendment unless it may deny the request under applicable law.

_____ _____
Signature Date

Please note: Applicable law requires us to respond to you within 60 days after receiving your request, unless we send you notification that we will need an additional 30 days to respond.

For office use only:
Received by: _____ Date: _____

GRANT OF AMENDMENT OF PHI REQUEST

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for amendment of your own protected health information (PHI) on **[date]**.

We have agreed to comply with your request. Accordingly, we will **[append or link the corrected information to the PHI in our possession]**.

If you like, we will notify persons you believe have received the PHI that is the subject of your amendment request. Please fill out and return the enclosed form listing the names and, if known, addresses, of those persons or entities. Please note that you must sign the form, giving us written permission to disclose this amended information to the people you have listed.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Sincerely,

[Name]
[Title]

Enclosure

NOTIFICATION OF ADDITIONAL TIME TO RESPOND TO AMENDMENT OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for an amendment to your own protected health information (PHI) on **[date]**. We have been unable to respond due to **[give reason for delay]**. We will respond to your request by **[specific date no more than 30 days from original due date of response]**.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Thank you for your patience.

Sincerely,

[Name]
[Title]

DENIAL OF REQUEST FOR AMENDMENT OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

Dear **[participant, beneficiary, or personal representative]**:

We have reviewed your request for amendment of your own protected health information (PHI). Your request is denied for the following reason:

_____ We believe the records identified in your request are accurate and complete.

_____ **[Part of the <or> The]** information you requested is not contained in our designated record sets. This means that we do not use the information you requested to make decisions relating to your health benefits. Accordingly, we are not required to amend it under the federal Privacy Rule.

_____ We did not create the records identified in your request. If you believe the person or entity that created the record is no longer available to respond to a request for amendment, please notify us and we will reconsider your request.

_____ We have determined that the records you identified in your request would not be available for inspection under the "right of access" provisions of the federal Privacy Rule, and therefore are not subject to amendment.

If you disagree with our denial, you may submit a written statement setting forth the basis for your disagreement. Your statement may be no longer than **[1 page].** If you choose not to file a statement of disagreement, you may ask that we include your request for amendment and our denial of your request with any future disclosures of the records at issue. If you wish to pursue either option, please submit in writing (1) your statement of disagreement, or (2) your request that we include in future disclosures your amendment request and our denial of that request to:

[Name]
[Address]

You may submit a complaint about this denial to us. If you choose to do so, please direct your complaint as indicated below. Please note that your complaint is not considered an appeal of our denial.

[Name of the Health Plan designated complaint contact person/office]
[Address]
[Telephone number]

You may also submit a complaint about this denial to the head of the U.S. Department of Health and Human Services. Your complaint must be in writing, either on paper or electronically, and must include the following information: (1) our name, and (2) a description of the acts or omissions that you believe violate our responsibilities under the Privacy Rule. Your complaint must be filed within 180 days of the date of this letter.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Sincerely,

[Name]
[Title]

NOTICE TO OTHERS OF AMENDMENT OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

Dear **[person or entity in possession of amended protected health information (PHI)]:**

Please note that you may have in your records the following protected health information (PHI) relating to **[name of participant or beneficiary]**:

[description of PHI]

We have amended that PHI as follows:

[describe amendment]

Please make a note of it in your records. This notice is being given as required by 45 CFR § 164.526, which is part of the Privacy Rule issued by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

[Add when notice goes to a business associate.] Under your contract with us, you are a business associate, and as such are required to append or link this notice or, if you choose, the amendment described above, to the PHI described.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Sincerely,

[Name]
[Title]
[Name Health Plan]

REQUESTOR'S LIST OF PERSONS OR ENTITIES TO BE NOTIFIED OF AMENDMENT

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

PERSONS OR ENTITIES TO BE NOTIFIED OF AMENDMENT

I authorize the Health Plan to notify the persons or entities listed below of the amendment the Health Plan has made to my protected health information (PHI).

NAME OF PERSON OR ENTITY	**ADDRESS**

(Please attach additional pages, if needed.)

Date: _____ Signature: _____

Printed name: _____

Please submit this form to**: [Title] [Address]**

AMENDMENT REQUEST TRACKING LOG

Please note: This Administrative Form relates to the Health Plan's Policy Form 7, Amendment of the PHI.

Requestor	Date Rec'd	Extension	Granted	Denied[2]	Records amended?	Others Notified

[2] Please indicate the following reason for denial: (a)-information is accurate and complete; (b)-information not created by the Health Plan; (c)-information not in designated records sets; (d)-information not subject to the right of access; (e)-requestor not authorized personal representative; (f)-other.

Accounting of Disclosures of PHI

Policy Statement

Individuals have the right to receive an accounting of disclosures of protected health information (PHI) made by the Health Plan, including any business associate on behalf of the Health Plan.

Policy Interpretation and Implementation

Request for an Accounting of Disclosures of PHI

1. An individual or his/her representative may request an accounting of disclosures of his/her PHI made by the Health Plan, including any business associate on behalf of the Health Plan, during a specified time period of up to six (6) years prior to the date of the request of an accounting. Disclosures must be tracked by the Health Plan for purposes of an accounting except the following disclosures:

    a. To carry out treatment, payment or healthcare operations (TPO) as permitted under current law;

    b. To the individual about his/her own PHI;

    c. To persons involved in the individual's care;

    d. For national security purposes;

    e. Pursuant to the individual's authorization;

    f. To federal/health department officials as permitted under current law; and

    Notwithstanding the foregoing, the Health Plan shall be required to provide an accounting only of those disclosures identified in the governing regulations under HIPAA.

Time Frame of Accounting Reports

2. Other than the exceptions noted above, the accounting record must include disclosures of PHI that occurred during the six (6) years (or such shorter time period as is specified in the request or as is provided under HIPAA) prior to the date of such request, including disclosures made by or to any of the Health Plan's business associates.

Content of Accounting of Disclosures Record

3. The content of the written accounting of disclosures record must contain, at a minimum, the following information:

    a. Date of the Name of the entity or individual who received the PHI disclosure;

    b. The address of the person receiving the PHI (if known)

    c. A brief description of the PHI disclosed; and

    d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu thereof,

a copy of the individual's authorization or the request for the disclosure.

Multiple Disclosures

4. If, during the time period for the accounting, *multiple* disclosures have been made to the same entity or individual for a single purpose, or pursuant to a single authorization, the accounting may provide the information as set forth in paragraph 3 above for the first disclosure, and then summarize the frequency of number of disclosures made during the accounting period and the date of the last disclosure during the accounting period.

Time Frame for Providing Accounting of Disclosure Data

5. An individual's request for an accounting of PHI disclosures must be provided to the individual or representative within sixty (60) days of such request. If unable to provide the accounting within the sixty (60) day time frame, a one time thirty (30) day extension may be provided if:

   a. The individual is notified in writing of the delay;

   b. The notice includes the reason(s) why the delay is necessary; and

   c. The notice includes the date by which the accounting will be provided.

Log

6. The Health Plan will keep a log of all disclosures required by paragraph 1 above which will include all necessary information.

Record Retention

7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

8. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

9. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except

holidays at 218-894-2439 x1035.

Violations

10. Violations of this policy will be subject to discipline.

Effective Date

11. July 1, 2014.

References:
45 C.F.R. § 164.528

REQUEST FOR AN ACCOUNTING OF DISCLOSURES

Please note: This Administrative Form relates to the Health Plan's Policy Form 8, Accounting of Disclosures of PHI.

You have a right to request that the Health Plan provide you with an accounting of certain disclosures that it has made of your protected health information (PHI). Please see the Health Plan's Notice of Privacy Practices **[<optional> or contact the Health Plan's Privacy Officer at xxx-xxx-xxxx]** for information.

Please submit this form to: **[Title]**
[Address]

Your name: _____

Address: _____

Daytime phone number: _____

Please select one:

___ I participate in or am covered under the Health Plan **[name of health plan(s)]**.

___ I am the personal representative of an individual participating in or covered under the Health Plan **[name of health plan(s)]** (*please attach proof of personal representative status*).

I would like an accounting of covered disclosures of my PHI made by the Health Plan between the following dates:

_____ and _____.

Note: We are not required to provide an accounting of disclosures we made prior to the effective date of the federal privacy rules (April 14, 2003) **[if small group health plan: (_____)]**.

Please Read Carefully and Sign

I understand that the Health Plan will provide the requested accounting of disclosures if required to do so under applicable law. If this is not my first request for an accounting within a 12-month period, I understand that the Health Plan will notify me of its reasonable costs for complying with my request and provide me with the opportunity to agree to pay those charges in order to receive the requested accounting.

_____ _____
Signature Date

Please note: Applicable law requires us to respond to you within 60 days after receiving your request, unless we send you a notification that we will need an additional 30 days to respond.

For office use only:
Received by:_____ Date:_____

ACCOUNTING OF DISCLOSURES OF PHI

Please note: This Administrative Form relates to the Health Plan's Policy Form 8, Accounting of Disclosures of PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for an accounting of disclosures of your protected health information (PHI) on **[date]**. We **[set forth below] <or> [enclose]** an accounting of those disclosures that, by law, must be provided in response to your request.

Information Disclosed	**Date Disclosed**	**Disclosed To:**	**Purpose of Disclosure**
	[Note: For multiple disclosures to the same entity, include all information for first such disclosure, how often or when subsequent disclosures were made, and the date of the last disclosure.]	[Note: Include contact information, if known.]	[Note: If disclosure was made pursuant to a written request, you may include copies of the written request instead of describing the purpose of the disclosure.]

There is no charge for this accounting. However, if you request additional accountings within the next 12 months, there may be a charge to you for our costs in complying with your requests.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Sincerely,

[Name]
[Title]

NOTIFICATION OF ADDITIONAL TIME TO RESPOND TO ACCOUNTING REQUEST

Please note: This Administrative Form relates to the Health Plan's Policy Form 8, Accounting of Disclosures of PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for an accounting of disclosures of your protected health information (PHI) on **[date]**. We have been unable to respond due to **[give reason for delay]**. We will respond to your request by **[specific date no more than 30 days from original due date of response]**.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Thank you for your patience.

Sincerely,

[Name]
[Title]

NOTIFICATION OF CHARGES FOR SECOND REQUEST IN 12 MONTH PERIOD

Please note: This Administrative Form relates to the Health Plan's Policy Form 8, Accounting of Disclosures of PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request for an accounting of disclosures of your protected health information (PHI) on **[date]**. We responded to a prior request from you for an accounting on **[date]**. You are entitled to one accounting without charge during any 12 month period. Because this is your second request within 12 months, we will charge you **[$___]** for our reasonable costs in putting together the accounting. These costs include the time and expense of reviewing our records.

If we do not hear from you within **[30] days** from the date of this letter, we will assume that you have withdrawn your request. If you do not wish to withdraw your request, please sign the acknowledgement at the bottom of this letter and return it within **[30] days**.

[Please call us at xxx-xxx-xxxx if you have any questions.]

Thank you for your patience.

Sincerely,

[Name]
[Title]

ACKNOWLEDGMENT

I, _____, understand that I am being charged $____ for my most recent request for an accounting of disclosures of my protected health information (PHI) because I have requested more than one accounting within a 12 month period. I agree to pay all reasonable charges prior to receiving the accounting. A check or money order is enclosed.

_____	_____
Name (print)	Signature
_____	_____
Telephone Number	Date

Return acknowledgement to**: [Title] [Address]**

ACCOUNTING REQUEST TRACKING LOG

Please note: This Administrative Form relates to the Health Plan's Policy Form 8, Accounting of Disclosures of PHI.

Name of Requestor [and ID Number]	Date Rec'd	Request Forwarded to Business Associates	Notification of Charges (more than one request in 12 months)	Acceptance of Charges Rec'd	Extension	Accounting Provided

DISCLOSURE TRACKING LOG

Please note: This Administrative Form relates to the Health Plan's Policy Form 4 (Use or Disclosure of PHI) and Policy Form 20 (Disclosures to Plan Sponsor).

Requestor's Name & Address	Date Received	Purpose of Disclosure	Information Disclosed	Date Disclosed	Disclosed By	Method of Verification

Verification Prior to Disclosure of PHI

Policy Statement

Prior to disclosing PHI, including electronic protected health information (ePHI), the Health Plan must verify the identity of the recipient and the recipient's authority to have access to PHI, unless the identity and authority are known to the Health Plan. In addition, when it is a condition of disclosure, prior to the disclosure of PHI, the Health Plan must obtain any documentation, statements, or representations of the recipient as required by the Privacy Rule.

Please note: This Policy relates to Form 4, Use and Disclosure of PHI, Form 6, Individual's Right to Access & Copy PHI, and Form 19, Disclosures to the Plan Sponsor.

Policy Interpretation and Implementation

Responsibility For Obtaining Verifications

1. The HIPAA Privacy Officer or his/her designee will be responsible for obtaining verifications when disclosure of PHI is necessary.

Verification of Identity and Authority

2. Before releasing PHI, sufficient information must be obtained from the person requesting the information to reasonably conclude, under the circumstances, that the person is who he/she says he/she is and has authority to have access to the PHI. The type of information required will depend on the nature of the request, from whom it is made, and the method in which it is made.

Request for Information In Person

3. When a request for PHI is made in person, identity may generally be verified by inspecting some form of photo identification. If photo identification is unavailable, identity may be verified by inspection of some other form of government issued identification.

   In addition, in cases of disclosure for public policy purposes, authority to have access to PHI may generally be verified by receipt of the full name, date of birth, and one other additional piece of information (i.e., SSN, other identification number, address, or telephone number) of the subject of the PHI and:

   a. A written statement of the authority under which the PHI is requested (or if a written statement is impracticable, an oral statement); or

   b. A legal document, such as a warrant, subpoena, court order, or other legal process.

Request for Information By Telephone

4. When a request for PHI is made by telephone, identity may generally be verified by receipt of information that identifies the person requesting the information. For instance, if the person requesting the PHI is the subject of the PHI, then identity may be established by providing his/her full name, date of birth, and one other additional piece of information (i.e., SSN, other identification number, address, or telephone number). When the person requesting the information is a third party (i.e.

health care provider), identity may be established by obtaining the caller's telephone number and calling him/her back, making sure the area code and exchange matches a listed telephone number for the company/agency. In order to verify authority to access the PHI when it is requested by someone other than the subject, obtain the full name, date of birth, and one other additional piece of information (i.e., SSN, other identification number, address, or telephone number) regarding the subject of the PHI and a statement of the authority under which the PHI is requested.

Please note: The Health Plan is not required to release PHI when the request for release is made by telephone.

Request for Information By Mail or Email

5. If a request for PHI is received by mail, identity may generally be verified by receipt of some unique piece of information that identifies the person requesting the information or by receipt of the request in a format that tends to establish the identity of person making the request. For instance, if the person requesting the PHI is the subject of the PHI, then a written request containing the person's social security number or other unique identification number will be sufficient. When the person requesting the information is a health care provider or a public agency, receipt of the request on appropriate letterhead will be sufficient.

Verification of Documentation, Statements, or Representations

6. The person verifying the documentation, statements, or representations provided by the recipient as required by the Privacy Rule may, when doing so is reasonable under the circumstances, rely on documentation, statements, and representations that, on their face, meet the applicable requirements. Such reliance will not be reasonable when information is known by the person that tends to indicate the documentation, statement, or representation is not authentic. In such situations, additional steps to verify the authenticity of the documentation, statement, or representation shall be taken.

Log

7. The Health Plan will keep a log of all verifications, which will include all necessary information.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

9. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the

HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

10. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

11. Violations of this policy will be subject to discipline.

Effective Date

12. July 1, 2014.

References:
45 C.F.R. § 164.508(b)

DISCLOSURE TRACKING LOG

Please note: This Administrative Form relates to the Health Plan's Policy Form 4 (Use or Disclosure of PHI), Policy Form 20 (Disclosures to Plan Sponsor), and Policy Form 9 (Verification Prior to Disclosure of PHI).

Requestor's Name & Address	Date Received	Purpose of Disclosure	Information Disclosed	Date Disclosed	Disclosed By	Method of Verification

Individual Requested Restrictions on Use or Disclosure of PHI

Policy Statement

Individuals have the right to request restrictions on uses and disclosures of protected health information (PHI), including electronic protected health information (ePHI), relative to treatment, payment, or health care operations (TPO).

Policy Interpretation and Implementation

Request for Restriction on use or Disclosure of PHI

1. A request for restriction of use or disclosure of information must be submitted in writing to the HIPAA Privacy Officer. Such request must specify the type of information to be included in the restriction and to whom the restriction applies.

2. Upon receipt of an individual's request that a restriction be placed on the use or disclosure of PHI, the HIPAA Privacy Officer will:

   a. Determine the reasonableness of the request based on the administrative capability of the Health Plan to comply with such request;

   b. Identify the means and location the individual wishes the information to be communicated; and

   c. Notify the individual whether or not the Health Plan agrees to the restriction within sixty (60) days of the date of such request unless an extension is necessary. Such extension will not exceed thirty (30) days.

   Notwithstanding the foregoing, in accordance with and as required by HIPAA (as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH")), the Privacy Officer will agree to the individual's request (1) if it relates to the disclosures of PHI to a health plan for the purpose of carrying out payment or health care operations, and (2) if the restriction applies to PHI that pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

Exceptions to Restrictions

3. Should the Health Plan agree to the restriction, the Health Plan and its business associates will honor such request except when:

   a. The restriction is terminated by the Health Plan or the individual, and/or

   b. There is an emergency treatment situation.

   The HIPAA Privacy Officer will be responsible for notifying any impacted business associates.

Emergency Treatment

4. When emergency treatment is necessary, the provider of the treatment may not use or disclose PHI or information which a restriction has been placed, except for what is necessary to provide appropriate emergency care for the individual. The emergency health treatment provider may not further disclose the restricted information beyond what is needed for the emergency treatment.

Termination of a Restriction

5. The Health Plan may terminate a restriction:
   a. When the individual requests the termination; and/or
   b. When the Health Plan informs the individual of the termination.

Termination Notices

6. Termination notices must be in writing and must indicate the effective date such termination and the reason(s) for such termination.

Record Retention

7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

8. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. July 1, 2014.

References:
45 C.F.R. § 164.522

REQUEST TO RESTRICT CERTAIN USES AND DISCLOSURES

Please note: This Administrative Form relates to the Health Plan's Form 10, Individual Requested Restrictions on Use or Disclosure of PHI.

You have a right to request the Health Plan restrict:

- Uses or disclosures of your protected health information (PHI) in carrying out payment or health care operations activities.
- Disclosures to family members or friends involved in your health care or payment relating to your health care.

Use this form to request such a restriction. **THE HEALTH PLAN IS NOT REQUIRED TO COMPLY WITH YOUR RESTRICTION REQUEST UNLESS (1) IT RELATES TO THE DISCLOSURES OF PHI TO A HEALTH PLAN FOR THE PURPOSE OF CARRYING OUT PAYMENT OR HEALTH CARE OPERATIONS, AND (2) THE RESTRICTION APPLIES TO PHI THAT PERTAINS SOLELY TO A HEALTH CARE ITEM OR SERVICE FOR WHICH THE HEALTH CARE PROVIDER INVOLVED HAS BEEN PAID OUT OF POCKET IN FULL.**

IMPORTANT: IF YOU BELIEVE YOU WILL BE ENDANGERED IF YOUR PHI IS DISCLOSED THROUGH A COMMUNICATION WE MIGHT MAKE TO YOU OR SOMEONE IN YOUR HOUSEHOLD, PLEASE SUBMIT THE FORM ENTITLED "REQUEST FOR CONFIDENTIAL COMMUNICATION."

Please submit this form to**:** **[Title]**
[Address]

Your name: _____

Address: _____

Daytime phone number: _____

<u>Please select one</u>:

___ I participate in or am covered under the Health Plan **[name of health plan(s)]**.

___ I am the personal representative of an individual participating in or covered under the Health Plan (*please attach completed Designation of Personal Representative form*).

___ I request the Health Plan to restrict its uses or disclosures of my PHI for purposes of payment or health care operations. Specifically, I request the following restrictions (describe):

(If more space needed, please attach separate sheet)

___ I request the Health Plan to not make disclosures to the following family members or friends who may be involved in my health care or payment with respect to my health care (list names):

(If more space needed, please attach separate sheet)

Please Read Carefully and Sign

I understand that the Health Plan is not required to agree to my requested restriction. I also understand that if the Health Plan agrees to the requested restriction, it may stop doing so prospectively so long as it informs me that the restriction is removed.

_____ _____

Signature Date

For office use only:

Received by:_____ Date:_____

RESPONSE TO REQUEST TO RESTRICT CERTAIN USES AND DISCLOSURES

Please note: This Administrative Form relates to the Health Plan's Policy Form 10, Individual Requested Restrictions on Use or Disclosure of PHI.

Dear **[participant, beneficiary, or personal representative]**:

We received your request that we restrict certain uses and disclosures of your protected health information (PHI). As you know, except in limited cases, the law does not require us to agree to your requested restriction.

_____ We **will not** be able to agree to your restriction. However, if you believe you will be endangered if your PHI is disclosed through a communication we might make to you or someone in your household, please submit the form entitled "Request For Confidential Communication."

_____ We **will** agree to restrict uses and disclosures of your PHI as you requested. Specifically, **[describe uses and disclosures that will not be made, including specifically the names of family members/friends to whom disclosures will not be made.]**

Please note that we may remove this restriction prospectively at any time upon providing notice to you.

[<Optional> Please call us at xxx-xxx-xxxx if you have any questions.]

Sincerely,

[Name]
[Title]

Individual Requested Restrictions on Confidential Communications

Policy Statement

Individuals have the right to request an alternate means of communication of the individual's protected health information (PHI), including electronic protected health information (ePHI), from the Health Plan to the individual. The restrictions apply only to communications to the individual by the Health Plan or communications that would otherwise go to the subscriber of the policy under which the individual has coverage. The effect of this is to ensure a family member who is not the subscriber can receive communications of PHI at the individual's workplace or other alternate address or phone number, so that other family members are unaware of the information.

Policy Interpretation and Implementation

Request for Confidential Communications

1. A request for confidential communications must be submitted in writing to the HIPAA Privacy Officer. Such request must specify the type of information to be covered by the confidential communication's restriction, and to whom the restriction applies, the alternate address or other method of contact requested, and how payment will be handled (if applicable). The Health Plan may require evidence that if the information is disclosed other than the manner requested it could endanger the individual.

Consideration of Request

2. Upon receipt of an individual's written request for confidential communications of PHI, the HIPAA Privacy Officer will:
    a. Determine the reasonableness of the request based on the administrative capability of the Health Plan to comply with such request;
    b. The determination of reasonableness will not include an evaluation of the merits of the individual's reason for making the request;
    c. Identify the alternate means by and/or location to which the individual requests the information to be communicated and how payment will be handled; and
    d. Notify the individual whether or not the Health Plan agrees to the request within sixty (60) days of the date such request was received unless an extension is necessary. Such extension shall not exceed thirty (30) days.

Exceptions to confidential communications

3. Should the Health Plan agree to the confidential communications, the Health Plan and its business associates will honor such request except when the confidential communication request is terminated by the Health Plan or the individual. The HIPAA Privacy Officer will be responsible for notifying any impacted business associates.

Termination of confidential communications

4. The Health Plan may terminate confidential communications:
   a. When the individual requests the termination; and/or
   b. When the Health Plan informs the individual of the termination.

Termination Notices

5. Termination notices must be in writing and must indicate the date such termination is to become effective and the reason(s) for such termination. The termination notice must be provided before the effective date of the termination notice. A copy of the termination notice must be filed in the individual's records maintained for HIPAA purposes.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

8. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. July 1, 2014.

References:
45 C.F.R. § 164.522(b)

REQUEST FOR CONFIDENTIAL COMMUNICATIONS

Please note: This Administrative Form relates to the Health Plan's Policy Form 11, Individual Requested Restrictions on Confidential Communications.

You have a right to request that the Health Plan provide alternative means or alternative locations for you to receive communications of your protected health information (PHI). We must agree to your request for a confidential communication **only** if (1) you provide a reasonable alternative means or locations for the communication, and (2) you believe that a disclosure of the information could endanger you.

Please submit this form to**:** **[Title]**
[Address]

Your Name: _____

Address: _____

Daytime phone number: _____

<u>Please select one</u>:

___ I participate in or am covered under the Health Plan **[name of health plan(s)]**.

___ I am the personal representative of an individual participating in or covered under the Health Plan **[name of health plan(s)]** (*please attach completed Designation of Personal Representative form*).

My request for confidential communications from the Health Plan applies to the following types of communications (list):

(If more space is needed, please attach a separate sheet)

The communications identified above should be made to me in the following manner (please provide an alternative address, telephone number, or e-mail address):

Please Read Carefully and Sign

I believe that disclosure of my PHI in the communications described above could endanger me. I understand that the Health Plan is not required to agree to my request for a confidential communication if I do not provide a reasonable alternative means for the communications or if I do not believe that the disclosure of information in the communication will endanger me.

_____ _____

Signature Date

For office use only:

Received by:_____ Date:_____

RESTRICTED USES AND CONFIDENTIAL COMMUNICATION REQUEST TRACKING LOG

Please note: This Administrative Form relates to the Health Plan's Policy Form 10 (Individual Requested Restrictions on Use or Disclosure of PHI) and Policy Form 11 (Individual Requested Restrictions on Confidential Communications).

Requestor	Date Rec'd	Restricted Use	Confidential communication	Request Fulfilled	Communicated to Business Associates	Comments

Privacy Complaint Procedure

Policy Statement

Individuals, family members, employees, the general public, or business associates have the right to file complaints regarding Health Plan policies, procedures, or practices relative to the access, use, or disclosure of protected health information (PHI), including electronic protected health information (ePHI).

Policy Interpretation and Implementation

Designation of Person to Receive Complaints

1. The HIPAA Privacy Officer has been designated as the individual responsible for receiving, processing, and investigating all privacy related complaints. The HIPAA Privacy Officer may in turn designate employees in particular areas to assist.

Filing of Privacy Complaints

2. Any individual, representative, family member, employee, business associate, visitor, or the general public may file a grievance or complaint regarding Health Plan privacy practices (e.g., denial of access to PHI, amendment of health records, problems with business associates, HIPAA policy and procedure violations, etc.) without fear or reprisal or retaliation in any form.

Submitted Complaints

3. Complaints should be submitted to the HIPAA Privacy Officer in writing.

Investigation Process

4. The HIPAA Privacy Officer or his/her designee will begin an investigation into allegations within five (5) working days of the receipt of the complaint.

Results of Investigation

5. A written report of the findings of the investigation will be provided to the individual filing the complaint within thirty (30) days of receiving such complaint unless an extension is necessary to complete the investigation. Such extension may not exceed thirty (30) days.

Dissatisfaction of Investigation/Resolution

6. Should the individual not be satisfied with the result of the investigation, or the recommended resolution(s), he/she may file a complaint with the Secretary of Health and Human Services (HHS).

Filing Complaints with the Secretary of HHS

7. Complaints may be filed directly with the Secretary of HHS. Such complaints must be in writing, identify the Health Plan, and must describe the violation. Complaints must be filed within one-hundred eighty (180) days of the complainant learning of the alleged violation or should have been aware of the alleged violation.

Address of Secretary of HHS

8. The address of the Secretary of HHS is located in the Notice of Privacy Practices (NPP) and/or made available to individuals. Persons may also obtain the address from the HIPAA Privacy Officer.

Retention of Complaints Log

9. The HIPAA Privacy Officer or his/her designee will maintain a log of all complaints received. Copies of all complaints, their disposition and resolutions, and our complaint log will be maintained for a period of at least six (6) years from the date such complaint was received.

Record Retention

10. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

11. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

12. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

12. Violations of this policy will be subject to discipline.

Effective Date

13. July 1, 2014.

References:
45 C.F.R. § 164.530(d)

PRIVACY COMPLAINT FORM

Please note: This Administrative Form relates to the Health Plan's Policy Form 12, Privacy Complaint Procedure.

You have a right to file a complaint about the Health Plan's privacy practices or the Health Plan's compliance with the Notice of Privacy Practices, Privacy Policies and Procedures, or the federal Privacy Rule. The Health Plan will not require you to waive any right you may have under the federal Privacy Rule to file your complaint, nor will filing your complaint adversely affect your enrollment in the Health Plan, your eligibility for benefits under the Health Plan, or payment of your claims under the Health Plan.

Please submit this form to: **[Title]**
[Address]

Your name: _____

Address: _____

Daytime phone number: _____

Please provide a concise statement of your complaint:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Date: _____ Signature: _____

Printed name: _____

For office use only:
Received by: _____ Date: _____

RESPONSE TO PRIVACY COMPLAINT

Please note: This Administrative Form relates to the Health Plan's Policy Form 12, Privacy Complaint Procedure.

Dear **[participant, beneficiary, or personal representative]**:

We received your complaint regarding the Health Plan's handling of your protected health information (PHI). The privacy of PHI is important to us and we take it seriously.
You stated that **[brief description]**.

[We have investigated this matter and determined that no violation of our privacy policies and procedures or the Privacy Rule occurred.**] [Brief description of why use/disclosure was proper or policies/procedures are appropriate.]**

[We have investigated this matter and determined that a violation of **[brief description]** has occurred.**] [Brief description of what is being or has been done.]**

[Please call us at xxx-xxx-xxxx if you have any questions.]

Sincerely,

[Name]
[Title]

COMPLAINT TRACKING LOG

Please note: This Administrative Form relates to the Health Plan's Policy Form 12, Privacy Complaint Procedure.

Name of Individual Logging Complaint	Date Rec'd	Nature of Complaint	Covered Component[3]	Start Date of Investigation	Investigation Completion Date	Date Response Issued to Individual Logging Complaint	Action Taken

[3] For covered entities who are a part of an Organized Health Care Arrangement (OHCA), record which covered component is affected by the complaint.

Authorization for Use or Disclosure of PHI

Policy Statement

All uses and disclosures of protected health information (PHI), including electronic protected health information (ePHI), beyond those otherwise permitted by current HIPAA law, and not otherwise prohibited under another applicable law, require a signed authorization. In addition, the Health Plan, including any business associates on behalf of the Health Plan, may choose to obtain a signed authorization in situations where it is not required.

Policy Interpretation and Implementation

Responsibility For Obtaining Authorizations

1. The HIPAA Privacy Officer or his/her designee will be responsible for obtaining authorizations when use or disclosure of PHI is necessary.

Provision of Treatment, Payment, or Eligibility

2. The provision of treatment, payment, or eligibility for benefits may not be conditioned on the individual's provision of an authorization for the use or disclosure of PHI.

Content of Authorization

3. Each authorization for the use or disclosure of an individual's PHI will be written in easy to read language and will include, at a minimum, the following information:
    a. A specific and meaningful description of the information to be used or disclosed;
    b. The name or identification of the person or class of person(s) authorized to make the use or disclosure;
    c. The name or identification of the person or class of person(s) to whom the requested use or disclosure may be made;
    d. An expiration date, condition or event that relates to the individual or the purpose of the use or disclosure; the authorization shall state that it will expire after ninety (90) days unless the individual has opted for a shorter or longer time. An individual may specify a longer period of time for the duration of the authorization only if the person:
        i. Is part of an approved research study and has given authorization for a longer period of time; or
        ii. Is expected to continue receiving services beyond ninety (90) days and has given authorization for a longer period of time, which may be up to one calendar year.
    e. A statement of the individual's right to revoke the authorization in writing, and exceptions to the

right to revoke, together with a description of how the individual may revoke the authorization. Upon written notice of revocation, further ruse or disclosure of PHI shall cease immediately except to the extent that the facility, program or individual has acted in reliance upon the authorization or to the extent that use or disclosure is otherwise permitted or required by law; (See policy entitled *Revocation of an Authorization.)*

f. A statement that the information may only be re-released with the written authorization of the individual, except as required by law;

g. The dated signature of the individual; and

h. If the authorization is signed by a personal representation of the individual, a description of the representative's authority to act on behalf of the individual.

Request Form

4. The Health Plan may develop a standard form for authorizing use and disclosure of PHI. If the Health Plan develops a form, the form must be used for all authorizations.

Requests to Use or Disclose PHI for Own Purposes

5. If the authorization is requested by the Health Plan for its own use or disclosure of the PHI it maintains, for purposes outside of treatment, payment or health care operations (TPO), health care oversight or public health activities, the following elements are required in addition to those specified in paragraph 3 above:

   a. Except in circumstances where it is allowed, a statement that treatment, payment and eligibility for benefits will not be conditioned upon the individual's provision of an authorization;

   b. A description of each purpose of the requested use or disclosure;

   c. A statement that the individual may refuse to sign the authorization;

   d. If applicable, a statement that the use or disclosure will result in direct or indirect remuneration for a third party; and

   e. A copy of the signed authorization provided to the individual.

Requests for PHI from Others

6. If the authorization is requested for disclosures of PHI by others, the following elements are required in addition to those specified in paragraph 5 above:

   a. A description of each purpose of the requested disclosure;

b. Except in circumstances where it is allowed, a statement that treatment, payment and eligibility for benefits will not be conditioned upon the individual's provision of an authorization;

c. A statement that the individual may refuse to sign the authorization; and

d. A copy of the signed authorization provided to the individual.

Use or Disclosure of PHI for Research

7. Use or disclosure of PHI created for research generally requires an authorization unless such use or disclosure is permitted by law. Such authorization must include the basic elements specified in paragraphs 3, 5, and 6 above, as well as the following information:

   a. A description of the extent to which PHI will be used to carry out TPO;

   b. A description of any PHI that will not be used or disclosed for purposes otherwise permitted, provided that the limitation may not preclude disclosures required by law or to avert serious threat to health or safety; and

   c. References to any privacy notice expected to be given to the individual, which must include statements that the terms outlined in the privacy notice are binding.

8. The authorization for the use and disclosure of PHI created for research may be combined in the same document with the consent to participate in research, or the privacy notice.

Sale of PHI

9. The exchange of PHI for direct or indirect remuneration requires an authorization, unless the sale is covered by a specific exemption contained in HIPAA. Such authorization must specifically state that the disclosure made pursuant to the authorization will result in remuneration to the Health Plan.

Use of PHI for Marketing

10. The use of PHI for marketing (as the term is defined in 45 C.F.R. Section 164.501) requires an authorization, unless the disclosure is covered by a specific exemption contained in HIPAA. If remuneration is provided to the Health Plan with respect to such marketing, the authorization must specifically state that remuneration is involved.

Record Retention

11. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

12. The HIPAA Privacy Officer is responsible for the

development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

13. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

14. Violations of this policy will be subject to discipline.

Effective Date

15. July 1, 2014.

References:
45 C.F.R. § 164.508

AUTHORIZATION FOR USE OR DISCLOSURE

Please note: This Administrative Form relates to the Health Plan's Policy Form 13, Authorization for Use or Disclosure of PHI.

Name: _____ Date: _____

I hereby authorize the use and disclosure of my protected health information (PHI) as indicated below. I understand that this authorization is voluntary and that I may revoke this authorization at any time except to the extent that action has been taken in reliance on this authorization. I also understand that if the individual or organization authorized to receive this information is not required to comply with current Privacy Rule, my PHI may be disclosed to others and no longer protected by the current federal Privacy Rule.

- ☐ Complete health care record(s)
- ☐ History & Physical Examination
- ☐ Laboratory Reports
- ☐ Medical/Treatment Records
- ☐ Pathology Reports
- ☐ X-Ray Reports
- ☐ Transcribed Reports
- ☐ Nurses' Notes
- ☐ Progress Notes
- ☐ Care Plans
- ☐ Dental Records
- ☐ Photographs, Video Tapes, Digital or other images
- ☐ Billing Statements
- ☐ Emergency Care Records
- ☐ Consultant Reports
- ☐ Discharge Summary

☐ Other: _____

The information checked and/or listed above is to be released to: _____, for the purposes of:

- ☐ Assisting with claims resolution
- ☐ Insurance or other benefit eligibility or coverage
- ☐ Litigation, potential litigation, or other adversarial proceedings
- ☐ Fitness for duty determination, drug testing results, or other employment-related purposes
- ☐ Other: _____

This authorization, for the release of the PHI checked and/or listed above, is valid for one (1) year after the date it is signed or upon completion of the use of the information for the purpose it was intended, unless an earlier expiration date is indicated here: _____.

I understand that the individual, organization, or entity receiving my PHI may receive financial or in-kind compensation in exchange for using or disclosing the PHI described above.

I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment or payment or my eligibility for benefits.

I understand that I may access and copy any PHI used or disclosed under this authorization. I understand that a fee may be charged for such copying services.

I hereby release the Health Plan, its employees, officers, and health care professionals from any legal responsibility or liability for disclosure of the above information to the extent indicated and authorized herein.

I understand that I may revoke this request at anytime by providing the Health Plan with my written notice of such revocation.

Date: _____	Signature: _____
	Printed name: _____
	or
Date: _____	Signature of personal representative: _____
	Printed name of personal representative: _____
	Relationship to me and basis upon which can sign: _____
	_____
	_____
Date: _____	Signature of witness: _____
	Printed name of witness: _____

Revocation of an Authorization

Policy Statement

Individuals have the right to revoke the authorization to access, release, use or disclose their protected health information (PHI), including electronic protected health information (ePHI), at any time. (Also see policy entitled: *Authorization for Use or Disclosure of PHI*.)

Policy Interpretation and Implementation

Revocation Request

1. All requests for revocation of an individual's authorization to access, release, use, or disclose PHI must be submitted to the HIPAA Privacy Officer in writing. The revocation must be specific enough to permit identification of the authorization that is being revoked. Oral requests will not be honored.

Notification of Personnel of a Revocation

2. Upon receipt of a written revocation, the HIPAA Privacy Officer will notify relevant staff and impacted business associates that a revocation has been received and that no further information may be released as specified in the authorization, with the exception that personnel may, as a result of relying on the authorization:

Exceptions to Revocation

   a. Complete the task it started (e.g., billings for services already provided); or,

   b. Submit findings from an independent medical examiner to the person/entity requesting it.

Record Retention

3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

4. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

5. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations	6. Violations of this policy will be subject to discipline.
Effective Date	7. July 1, 2014.

References:
45 C.F.R. § 164.508(b)(5)

REVOCATION BY SUBJECT OF PROTECTED HEALTH INFORMATION

Please note: This Administrative Form relates to the Health Plan's Policy Form 10 (Individual Requested Restrictions on Use or Disclosure of PHI), Policy Form 11 (Individual Requested Restrictions on Confidential Communications), Policy Form 13 (Authorization for Use or Disclosure of PHI), Policy Form 14 (Revocation of an Authorization), and Policy Form 18 (Personal Representative).

Name: _____ Date: _____

I hereby revoke the following authorization and/or restriction, effective immediately:

☐ Authorization for Use or Disclosure

☐ Designation of Personal Representative

☐ Requested Restriction on Use or Disclosure

☐ Request for Confidential Communications

☐ Other: _____

☐ Other: _____

☐ Other: _____

I understand that I cannot revoke any action already taken by the Health Plan in reliance upon my authorization and/or restriction prior to the date of this revocation.

I understand that this revocation removes all authorizations and/or restrictions previously in place, and if I want to impose future authorizations or restrictions regarding my PHI, I will have to submit a new completed form to the Health Plan.

Date: _____ Signature: _____

Printed name: _____

or

Date: _____ Signature of personal representative: _____

Printed name of personal representative: _____

Relationship to me and basis upon which can sign: _____

_____

_____

Date: _____ Signature of witness: _____

Printed name of witness: _____

For office use only:

Received by: _____ Date: _____

Business Associates & Business Associate Agreements

[HIPAA Privacy and Security]

Policy Statement

The Health Plan may disclose protected health information (PHI), including electronic protected health information (ePHI), to business associates, or allow business associates to create or receive PHI, provided the business associate executives sign a written agreement to appropriately safeguard such PHI.

Policy Interpretation and Implementation

Definition of Business Associate

1. A business associate, means a person or entity who is not an employee or workforce member of the Health Plan, who performs or assists in the performance of a function or activity on behalf of the Health Plan that involves the use or disclosure of PHI, or provides legal, actuarial, accounting, consulting, data compilation, management, administrative, accreditation, or financial services.

Definition of Employee/Workforce Member

2. An employee/workforce member, for the purposes of this policy, means any employee, trainee, volunteer, or any other person(s) whose conduct, in the performance of work for the Health Plan, is under the direct control/supervision of the Health Plan, regardless of payment source.

Identification of Business Associates

3. It is the Health Plan's obligation to ensure that all of the Health Plan's business associates have a written valid business associate agreement. The Health Plan shall use its best efforts to amend an existing business associate agreement as necessary to incorporate any new requirements imposed by HIPAA.

Content of Business Associate Agreements

4. The business associate agreement between the Health Plan and the business associate establishes permitted and required uses or disclosures of PHI. Pursuant to the agreement the business associate must agree to at least:
    a. Not use or disclosure PHI except as permitted by the agreement or as required by law;
    b. Develop and use safeguards to prevent unauthorized use or disclosure of PHI;
    c. Promptly report unauthorized access, use or disclosure of PHI, including a breach of unsecured ePHI, to the HIPAA Privacy Officer;
    d. Require any subcontractors to enter into a written agreement pursuant to which they agree to adhere to the same requirements as outlined in the agreement between the Health Plan and business associate;
    e. Make PHI available for access by the individual or

his/her representative as permitted by law;

f. Allow individuals to amend medical information and incorporate such amendments as part of the PHI;

g. Develop a process that allows for an accounting of uses and disclosures of PHI in accordance with current law;

h. To the extent the business associate is to carry out the Health Plan's obligation under the HIPAA privacy rules, comply with the requirements of the HIPAA privacy rules that apply to the Health Plan in the performance of such obligation;

i. Make its internal practices. books and records relating to its receipt or creation of PHI available to the Office of the U.S. Secretary of Health and Human Services for purposes of determining the Health Plan's compliance with HIPAA regulations;

j. Develop a process for returning or destroying all PHI upon termination of the business associate agreement;

k. Develop a process for continuing the full protection of PHI for as long as the business associate retains any PHI;

l. Implement administrative, physical and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI; and

m. Report to the Health Plan any "Security Incident" (as defined in 45 C.F.R. Section 164.304) of which business associate becomes aware with the frequency and in the level of detail and format as provided in the agreement.

n. Authorize termination of the agreement by the Health Plan if it determines the business associate has violated a material term of the agreement.

In addition, the business associate agreement may permit the business associate to use PHI received by it for the proper management and administration of the business associate and to carry out its legal responsibilities. The business associate agreement may also permit the business associate to disclose PHI for such purposes if (i) the disclosure is required by law, or (ii) the business associate receives reasonable assurances from the recipient of the PHI that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed and the recipient agrees to notify the business associate of any instances of

which it becomes aware in which the confidentiality of the PHI has been breached.

Breach of Business Associate Agreement

5. If the Health Plan knows of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligations under the agreement, the Health Plan will take reasonable steps to cure the breach or end the violation and, if such steps are not successful, will terminate the agreement, if feasible.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

8. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. July 1, 2014.

References:

45 C.F.R. § 164.504(e), 45 C.F.R. § 164.308(b), 45 C.F.R. § 164.314(a)

Retention of PHI Documentation

[HIPAA Privacy and Security]

Policy Statement

The Health Plan shall maintain all protected health information (PHI), including electronic protected health information (ePHI), documentation for a period of at least six (6) years from the date of its creation, or the date on which the document was last in effect, whichever is later.

Policy Interpretation and Implementation

Retention of PHI Documents

1. Certain documents classified as "privacy related documents" must be maintained for a period of at least six (6) years from the date of creation, or the date on which the document was last in effect, whichever is later.

Privacy Related Documents

2. "Privacy related documents" include:
    a. Documentation that identifies the:
        i. Name, telephone number and address of the Health Plan's HIPAA Privacy Officer and HIPAA Security Officer;
        ii. Name, title, telephone number and address of the individual responsible for receiving complaints;
        iii. Name, title, telephone number and address of the individual responsible for obtaining and processing requests for access, use, and disclosure of PHI;
        iv. Name, title, telephone number and address of the individual responsible for receiving and processing requests for amendment of PHI;
        v. Attempts to obtain consent when consent could not be obtained and the reason(s) why such consent could not be obtained;
        vi. Method by which PHI will be de-identified;
        vii. Sanctions imposed against Health Plan employees, business associates, or others who violate Health Plan policy/HIPAA regulations;
    b. All signed authorizations, consents, and agreed to restrictions;
    c. Copies of all notices of privacy practices (NPPs) including any revisions to such NPPs;
    d. Accounting of disclosures logs;

e. Any privacy complaints received and their dispositions; and

f. Copies of all HIPAA related policies and procedures.

Adding/Deleting Documentation

3. Documents may be added or deleted from the above listing as may become necessary by law or as may be established by Health Plan practice or policy.

Identifying/Storage of PHI Documents

4. The HIPAA Privacy Officer is responsible for identification and storage of privacy related records, electronic files, etc., for purposes of complying with this policy.

Record Retention

5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

6. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

7. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

8. Violations of this policy will be subject to discipline.

Effective Date

9. July 1, 2014.

References:
45 C.F.R. § 164.530(j)

HIPAA Privacy and Security Training Program

[HIPAA Privacy and Security]

Policy Statement

The Health Plan must train all relevant members of its workforce on HIPAA policies and procedures relating to privacy and security, as necessary and appropriate for the members of the workforce to carry out their function within the Health Plan.

Policy Interpretation and Implementation

HIPAA Training Program

1. To ensure the confidentiality of individual's protected health information (PHI), including electronic protected health information (ePHI), and to ensure the integrity and availability of ePHI, HIPAA training (HIPAA Training) shall be provided for all employees of the Plan Sponsor who have responsibilities involving the use/disclosure of PHI (including ePHI), and other workforce members as deemed necessary within the sole discretion of the HIPAA Privacy Officer and Security Officer. It is the responsibility of the HIPAA Privacy Officer and Security Officer to oversee such HIPAA Training.

Workforce Members

2. An employee/workforce member, for the purposes of this policy, means any employee, trainee, volunteer, or any other person(s) whose conduct, in the performance of work for the Health Plan, is under the direct control/supervision of the Health Plan, regardless of payment source.

Content of HIPAA Training Program

3. The HIPAA Training shall include, but is not limited to:

    a. An overview of the HIPAA privacy regulations relative to the identification and protection of PHI.

    b. A review of the Health Plan's HIPAA policies and procedures;

    c. A review of permissible uses and disclosures of PHI;

    d. Instruction regarding application of the Health Plan's HIPAA policies and procedures to employee's job responsibilities;

    e. Disclosure of the identity and location of the Health Plan's HIPAA Privacy Officer and Security Officer;

    f. A review of the requirement that all employees report any potential violations of the Health Plan's policies and procedures or the HIPAA regulations, and any security incidents, whether caused by a workforce member or a service provider, to the HIPAA Privacy Officer and Security Officer; and

g. A review of other information relative to the protection and security of PHI and ePHI.

Newly Hired Employees/ Business Associates

4. Before being allowed access to PHI, including ePHI, all newly hired employees, and employees new to a position requiring access to PHI, including ePHI, shall be required to sign and date a written acknowledgement that the new employee has completed HIPAA Training.

Acknowledgment of Training Attendance

5. Department directors will be required to have a signed and dated written acknowledgment that the new employee has completed HIPAA Training before being allowed access to PHI, including ePHI.

Attendance Records

6. The HIPAA Privacy Officer and Security Officer shall maintain a record of all personnel who attend HIPAA Training. Such records shall be maintained in accordance with the *Retention of PHI Documentation Policy*.

Methods and Means

7. Training may be accomplished through any reasonable means or combination of means including but not limited to live sessions, webinars, print materials, and may be conducted by the Plan Sponsor and/or an outside third party provider.

Annual Training

8. Updated training shall take place at least annually. Should a change in the training program or security systems occur before an annual training session occurs, impacted employees shall receive interim training materials or abbreviated instructions.

Record Retention

9. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

10. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

11. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except

holidays at 218-894-2439 x1035.

Violations 12. Violations of this policy will be subject to discipline.

Effective Date 13. July 1, 2014.

References:
45 C.F.R. § 164.530(b), 45 C.F.R. § 164.308(a)(5)

ACKNOWLEDGMENT OF TRAINING ATTENDANCE

Please note: This Administrative Form relates to the Health Plan's Policy Form 17, HIPAA Privacy Training Program.

I, _____, acknowledge that I have attended and completed HIPAA Training on _____, 20___.

_____ _____

Name (print) Signature

_____

Date

Personal Representative

Policy Statement

The Health Plan will treat a personal representative the same as it would the individual who is the subject of the protected health information (PHI), including electronic protected health (ePHI), unless one of the exceptions applies. In general, a personal representative is someone who is recognized under applicable state law as a personal representative (e.g., parent/guardian, power of attorney, executor of estate).

Policy Interpretation and Implementation

Designation as Personal Representative

1. The person who is the subject of the PHI may designate another person as a personal representative, or a person may seek to be recognized as a personal representative, by filing the appropriate written documentation with the Health Plan.

Rights of Personal Representative

2. The personal representative must be treated the same as the individual, except as specified below:

Restrictions on Personal Representative

   a. If the Health Plan reasonably believes that the individual has been or may be subjected to domestic violence, abuse, or neglect by the person seeking to be treated as a personal representative, or that treating the person as the personal representative could endanger the individual.

   b. If the Health Plan, in the exercise of professional judgment, decides that treating the person as the individual's personal representative would not be in the individual's best interest.

   c. If a parent is the personal representative of a minor child, but disclosure to the parent is prohibited under state law.

   d. If a minor child consented to the treatment, no other consent was required, and the minor has not requested the person be treated as the minor's personal representative.

   e. If a minor child may lawfully obtain treatment without the consent of a parent and consent was lawfully obtained.

   f. If the parent has agreed to a confidential relationship between the minor and the physician with respect to that treatment.

Record Retention

3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

4. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

5. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

6. Violations of this policy will be subject to discipline.

Effective Date

7. July 1, 2014.

References:
45 C.F.R. § 164.502(g)

DESIGNATION OF PERSONAL REPRESENTATIVE FORM

Please note: This Administrative Form relates to the Health Plan's Policy Form 18, Personal Representative.

Note: This form is used to confirm permission for the Health Plan to discuss with or disclose to a person's protected health information (PHI) to a particular individual who acts as the person's personal representative. Use of this information is strictly limited to that purpose.

Subject of PHI's Name: _____ Date: _____

Please complete either Part I or Part II below.

PART I: DESIGNATION BY SUBJECT OF PHI

I hereby authorize the following person to act as my personal representative as indicated below. I understand that this authorization is voluntary and that I may revoke this authorization at any time except to the extent that action has been taken in reliance on this authorization.

Name of personal representative:_____

Date of birth of personal representative (used for verification purposes on phone inquiries):_____

Social Security # of personal representative (used for verification purposes on phone inquiries):_____

Address:_____

Relationship to me:_____

Password personal representative must provide to access protected health information (PHI) about me:

Password:_____

Description of nature of representation and limits thereon (attach supporting documentation, if any, such as court orders, Power of Attorney, etc):_____

NOTE: I understand that I have the right to limit the information that is released under this authorization. For example, I may limit my personal representative's access to information about a particular issue. Any such limitations must be described below in writing. I understand that by leaving this section blank, I am imposing no limitations on disclosure.

Limitations on Disclosure:

_____

_____

_____

I understand that I may revoke this authorization at anytime by providing written notice of such revocation to the Health Plan.

I have had full opportunity to read and consider the content of this Designation of Personal Representative form. I confirm that this authorization is consistent with my request. I understand that, by signing this form, I am confirming my authorization that the Health Plan may use and/or disclose my PHI to the person named as personal representative for the purpose described above.

Date: _____	Signature: _____
	Printed name: _____
Date: _____	Signature of witness: _____
	Printed name of witness: _____

PART II: THIRD PARTY DESIGNATION

Name of personal representative: _____

Date of birth of personal representative (used for verification purposes on phone inquiries): _____

Social Security # of personal representative (used for verification purposes on phone inquiries): _____

Address: _____

Relationship to Subject of PHI: _____

Password personal representative must provide to access protected health information (PHI) about me:

Password: _____

Description of nature of representation and limits thereon (attach supporting documentation, if any, such as court orders, Power of Attorney, etc): _____

For office use only:
Received by: _____ Date: _____

Coordination with Other Laws

[HIPAA Privacy and Security]

Policy Statement

In addition to being subject to HIPAA, the Health Plan may also be subject to other state and federal laws regarding medical information and privacy and security. The Health Plan intends to comply with all applicable state and federal laws. However if there is a conflict between the laws, the HIPAA Privacy Officer or the HIPAA Security Officer, as the case may be, will resolve the conflict according to this Coordination with Other Laws policy.

Policy Interpretation and Implementation

Floor

1. The HIPAA regulations are the floor above which other laws may create more narrow restrictions. No law, whether federal or state, may allow less restriction than HIPAA.

Apply Both Laws

2. If a potential conflict exists, the Health Plan shall attempt to find a way to comply with both laws. For example, if one law permits disclosure, but HIPAA does not, the Health Plan could obtain an individual authorization and succeed in complying with both laws.

Follow the Law that Requires Use or Disclosure

3. If another federal law *requires* disclosure or use of PHI that HIPAA prohibits, the Health Plan may use or disclose the PHI in accordance with the other federal law. This is not a violation of HIPAA. HIPAA's privacy rules allow the Health Plan to use or disclose PHI as required by other federal laws.

Follow the More Specific Law

4. If there is a very specific law regarding use or disclosure of PHI including security of ePHI, and that law conflicts with HIPAA, the more specific law should be followed. For example, if HIPAA allows an individual a right to access test results, but a specific federal law prohibits that type of disclosure, the specific law should be followed.

State Law Preemption

5. HIPAA provides for preemption of state laws that are less restrictive than HIPAA. However, HIPAA does not preempt state laws that are more restrictive. If the Health Plan encounters a conflict between HIPAA and a state law, the Health Plan should follow the more restrictive law.

Record Retention

6. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

7. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies

and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

8. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

9. Violations of this policy will be subject to discipline.

Effective Date

10. July 1, 2014.

References:
Preamble to HIPAA Regulations

Disclosures to Plan Sponsor

[HIPAA Privacy and Security]

Policy Statement

The Health Plan may not disclose protected health information (PHI), including electronic protected health information (ePHI), to the plan sponsor except in specific situations recognized by HIPAA.

Policy Interpretation and Implementation

Definition of Plan Sponsor

1. The term "plan sponsor" means (i) the employer in the case of an employee benefit plan established or maintained by a single employer, (ii) the employee organization in the case of a plan established or maintained by an employee organization, or (iii) in the case of a plan established or maintained by two or more employers or jointly by one or more employers and one or more employee organizations, the association, committee, joint board of trustees, or other similar group of representatives of the parties who establish or maintain the plan.

Permitted Disclosure to Plan Sponsor for Settlor Functions

2. Summary health information may be disclosed to the plan sponsor for:
   a. Obtaining premium bids for providing health insurance coverage under the Health Plan; and
   b. Modifying, amending or terminating the Health Plan.

Summary Health Information

3. Summary health information is information that summarizes the claims history, expenses, or types of claims by individuals for whom the Plan Sponsor has provided health benefits under the Health Plan.

Amendment to Plan Document

4. Prior to the disclosure of PHI, including ePHI, by the Health Plan to the plan sponsor, the plan document must be amended as required by HIPAA and the plan sponsor must certify to the Health Plan such amendment has been made.

Permitted Disclosure to Plan Sponsor for Plan Administration Functions

5. To the extent described in the plan documents and notice of privacy practices, the Health Plan may disclose PHI, including ePHI, to the plan sponsor if such PHI or ePHI is needed to perform plan administration activities such as:
   a. Quality assurance;
   b. Claims processing;
   c. Auditing; and
   d. Monitoring and managing carve-out plans like vision and dental.

Enrollment Functions

6. These restrictions do not affect the plan sponsor's ability to perform enrollment functions on behalf of its employees.

Record Retention

7. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

8. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

9. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

10. Violations of this policy will be subject to discipline.

Effective Date

11. July 1, 2014.

References:

45 C.F.R. § 164.504(f); 45 C.F.R. § 164.314(b)(2)

Duty to Mitigate

[HIPAA Privacy and Security]

Policy Statement

The Health Plan will mitigate, to the extent practicable, any harmful effect that is known to the Health Plan of: (1) a violation of its policies and procedures by the Health Plan or its business associates, and (2) a security incident.

Policy Interpretation and Implementation

Mitigation Actions

1. When a violation of the Health Plan's policies and procedures or a security incident is brought to the attention of the Health Plan, the following action will be taken:
   a. The Privacy Officer and the Security Officer will be notified and the appropriate officer, depending on the nature of the violation or incident, will start an immediate investigation into the violation or incident;
   b. The Health Plan will identify the extent of the breach and will take reasonable steps to mitigate or correct the violation; and
   c. The Health Plan will document the steps taken to mitigate.

Security Incident Defined

2. "Security incident" is defined in 45 C.F.R. Section 164.304 and generally includes an attempted or successful access, use, disclosure, modification, or destruction of electronic protected health information (ePHI) in violation of the Health Plan's policies and procedures.

Record Retention

3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

4. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

5. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

6. Violations of this policy will be subject to discipline.

Effective Date

7. July 1, 2014.

References:
45 C.F.R. § 164.530(f); 45 C.F.R. § 164.308(a)

Discipline Policy

[HIPAA Privacy and Security]

Policy Statement

HIPAA requires the Health Plan to discipline individuals subject to, but who fail to comply with, HIPAA's requirements as reflected in the Health Plan's privacy and security policies and procedures. The purpose of this Discipline Policy is to establish guidelines for the disciplinary processes.

Please note: This Discipline Policy applies exclusively to violations of the Health Plan's privacy and security policies and procedures.

Policy Interpretation and Implementation

Discipline Policy

1. A failure to comply by an individual subject to the Health Plan's policies and procedures, or with the provisions of HIPAA, will be addressed in a timely manner. Specific disciplinary actions to be taken will be proportional to the severity of the infraction.

Initial Determination

2. Depending on the nature of the allegation, the HIPAA Privacy Officer or Security Officer, in its sole discretion, shall make an initial determination whether the allegations in the complaint constitute a violation of the Health Plan's privacy and security policies and procedures.

Discipline Procedure

3. Complaints or allegations against an individual will be discussed with the individual in question by the HIPAA Privacy Officer or Security Officer and, if deemed appropriate, will be investigated by the HIPAA Privacy Officer or Security Officer.

Known or Intentional Infraction

4. In general, a known or intentional infraction of the Health Plan's policies and procedures, or of HIPAA's provisions, will result in:

    a. First offense: Oral counseling by the HIPAA Privacy Officer or Security Officer, and written documentation in the individual's file.

    b. Second offense: Oral counseling by the HIPAA Privacy Officer or Security Officer, and a written warning.

    c. Third offense: Discipline up to and including probation, suspension or termination of employment.

Intentional Misuse

5. In general, intentional misuse or abuse of protected health information (PHI), including electronic protected health information (ePHI), will result in:
   a. First offense: Oral counseling by the HIPAA Privacy Officer or Security Officer, and written documentation in the individual's file.
   b. Second offense: Oral counseling by the HIPAA Privacy Officer or Security Officer, and a written warning.
   c. Third offense: Discipline up to and including probation, suspension or termination of employment.
6. Notwithstanding items 4 and 5, the HIPAA Privacy Officer and Security Officer retain discretion to deviate based on the particular facts and circumstances. Each infraction will be handled on an individual basis to ensure that disciplinary actions are proportional to the severity of the infraction.

Report to Authorities

7. The HIPAA Privacy Officer or Security Officer, in its sole discretion, may report a violation of the Health Plan's privacy and security policies and procedures to law enforcement and/or regulatory officials.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

9. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

10. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Effective Date 11. July 1, 2014

References:
45 C.F.R. § 164.530(e); 45 C.F.R. § 164.308(a)(1)

Administrative, Physical, and Technical Safeguards

[HIPAA Privacy and Security]

Policy Statement

The Health Plan will make reasonable efforts to maintain adequate administrative, technical and physical safeguards to protect the privacy of protected health information (PHI), including electronic protected health information (ePHI), from intentional or unintentional unauthorized access, use, or disclosure, theft, and unauthorized destruction, deletion, and alterations.

Policy Interpretation and Implementation

Implementation of Safeguards

1. The HIPAA Privacy Officer and the HIPAA Security Officer will work with appropriate personnel to determine and implement safeguards to protect PHI, including ePHI, from unauthorized access, use, or disclosure, theft, and unauthorized destruction, deletion, and alterations.

Periodic Review

2. The HIPAA Privacy Officer and HIPAA Security Officer will complete periodic reviews with all business units regarding the transportation, storage, usage, disclosure, and disposal of PHI, including ePHI, to identify risks to the privacy and security of the PHI. If necessary, policies and procedures will be amended and the applicable workforce retrained in order to maintain reasonable efforts of safeguarding such information.

Record Retention

3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

4. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

5. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439

x1035.

Violations

6. Violations of this policy will be subject to discipline.

Effective Date

7. July 1, 2014.

References:
45 C.F.R. § 164.530

Computer Terminals/Workstations

[HIPAA Privacy and Security]

Policy Statement

Computer terminals and workstations that are used to create, maintain, receive, or transmit protected health information (PHI), including electronic protected health information (ePHI), will be used and positioned in such a way that they are protected from inadvertent or intentional public view, view by those without a need to know, or unauthorized access.

Policy Interpretation and Implementation

Computer Terminals/ Workstations with Access to ePHI

1. Only the following computer terminals/workstations shall have access to ePHI: the computer terminals/workstations of the Privacy Office and Security Officer. In addition, mobile computer devices may also have access to ePHI, provided they are used solely by staff authorized to access protected health information (PHI), including ePHI. In limited circumstances, upon approval by the Security Officer, authorized staff may use a home workstation to access ePHI.

Location of Computer Terminals/Workstations

2. Insofar as practical/feasible, the computer terminals/workstations identified above shall be located in an area of the facility(ies) that may be secured and to which the public and unauthorized staff have limited access.

Positioning/Shielding Workstation/Terminals

3. Insofar as practical/feasible, the computer terminals/workstations identified above shall be positioned or shielded so that screens are not visible to the public and/or to unauthorized staff. When necessary, privacy screens shall be used to prevent screens from being viewed by the public and/or unauthorized staff.

Function of Computer Terminals/Workstations

4. The computer terminals/workstations identified above shall be used for administration of the Health Plan and, to the extent necessary, other human resources functions.

Access Limitations/Passwords

5. Only authorized users are granted access to PHI, including ePHI, and Health Plan information. Such access is limited to specific, documented and approved applications and level of access rights. To prevent unauthorized access, each authorized user shall be provided a unique username and password that must be used in order to access ePHI. Such usernames and passwords shall be periodically changed. Authorized users shall attempt to commit passwords to memory and, if not or until able to do so, take precautions against disclosure of written passwords to unauthorized staff and other third

parties.

Monitoring Access

6. Hardware, software and/or procedural mechanisms shall be implemented and used to track access and attempted access to workstations, systems, and programs containing ePHI. Such information shall monitored by the Security Officer on a regular basis for the purpose of identifying unauthorized access or attempted access.

Leaving Workstations or Terminals Unattended

7. A user may not leave his/her workstation or terminal unattended for long periods of time (e.g., breaks, lunch, meetings, etc.) unless the terminal screen is cleared and the user is logged off. Each user must log off at the end of his/her work shift.

Clearing Terminal Screens

8. A user must clear the terminal screen if the workstation or terminal is left briefly unattended. Each computer will have either password protected screen savers that will clear the terminal screen after a certain period of inactivity or an automatic log-out feature that will automatically log out a user after a certain period of inactivity.

Securing Hard Copy Data

9. All hard copy printed information must be positioned in such a manner that it cannot be viewed or read by the public and/or unauthorized staff. Such data must be placed in designated secure areas upon leaving the work area and at the end of the work shift.

Sharing/Piggyback of Password/User ID Code

10. A user may not (1) share or disclose his/her username and password or ID code with other staff members or other non-staff members, or (2) allow staff members or other non-staff members access privileges (e.g., piggyback access) while the user is logged onto the information system used by the Health Plan.

Mobile Computer Devices and Offsite Workstations

11. To the extent possible, the requirements of this policy shall apply to mobile computer devices (i.e., laptop computers, smartphones, etc.) and to offsite workstations (i.e., home offices).

Record Retention

12. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

13. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact

person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

14. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

15. Violations of this policy will be subject to discipline.

Effective Date

16. July 1, 2014.

References:

See generally 45 C.F.R. § 164.530, 45 C.F.R. § 164.310, 45 C.F.R. § 164.312.

Electronic Mail (E-Mail) and Internet System

[HIPAA Privacy and Security]

Policy Statement

The Health Plan utilizes electronic mail (E-Mail) in transmitting individual and Health Plan information. Authorized staff also have access to the internet. Established security measures must be followed by all personnel who have the authority to access, use, or transmit protected health information (PHI), including electronic protected health information (ePHI).

Policy Interpretation and Implementation

Application of Policies

1. This policy applies to all usage of e-mail systems related to the Health Plan whether or not the e-mail is originated from or is received into the computer or network system used by the Health Plan. The policy also applies to the usage of the internet system. Such policies apply to all authorized users including employees, business associates, staff or consultants.

Definition of Authorized User

2. For the purposes of this policy, an "authorized user" is defined as any person who (1) has been assigned a password and user ID code and (2) has the authority to read, enter, or update information created or transmitted by the Health Plan.

Personal Use or E-Mail and Internet Systems

3. Users have the responsibility and obligation to use e-mail and internet systems appropriately, effectively, and efficiently. Incidental personal use is permissible if:

    a. It is limited to meal and break times;

    b. It does not interfere with the normal business use of such services;

    c. It does not interfere with the work productivity of the user or other employees; and

    d. Passwords and user ID codes are not shared with others.

Improper Use of Health Plan's E-Mail or Internet Services

4. Improper use of e-mail and internet services is strictly prohibited. Examples of such improper use include, but are not limited to:

    a. Sending/forwarding harassing, insulting, defamatory, obscene, offending or threatening messages;

    b. Gambling, surfing or downloading pornography;

    c. Downloading or sending confidential individual

or PHI without proper authorization;

d. Copying or transmission of any document, software or other information protected by copyright and/or patent law, without proper authorization;

e. Transmission of highly sensitive or confidential information (e.g., HIV status, mental illness, chemical dependency, workers' compensation claims, etc.);

f. Obtaining access to files or communication of others without proper authorization;

g. Attempting unauthorized access to individual or Health Plan data;

h. Attempting to breach any security measure on any of the Health Plan's electronic communication system(s);

i. Attempting to intercept any electronic communication transmission without proper authorization;

j. Misrepresenting, obscuring, suppressing, or replacing an authorized user's identity;

k. Using e-mail addresses for marketing purposes without permission from the recipient(s);

l. Using e-mail system for solicitation of funds, political messages, or any other illegal activities; and/or

m. Releasing of passwords and user ID codes.

Protection Against Malicious Software

5. All information systems shall be equipped with up-to-date anti-virus software protecting the system against malicious software, including, but not limited to, viruses, Trojan horses, and worms. All authorized users shall be trained in the use of such software. Users of the information system must use extreme caution in downloading software from the internet and opening attachments to emails in order to protect against downloading malicious software. Software or attachments from unknown or untrustworthy sources shall not be downloaded or opened. The Security Officer shall be responsible for monitoring the anti-virus software to ensure it is up-to-date and to identify sources of malicious software.

Ownership of E-Mail Messages

6. Messages whether originated or received into the Health Plan e-mail system are considered to be the property of the Health Plan and, therefore, are

subject to the review and monitoring of the HIPAA Privacy Officer. The Health Plan reserves the right to access employee e-mail (whether present or not) for the purposes of ensuring the protection of individual/Health Plan information.

Inadvertent Access to E-Mail

7. During routine maintenance, upgrades, problem resolution, etc. information systems technician(s) may inadvertently access user e-mail communications. Such staff, when carrying out their assignments, will not intentionally read or disclose content of e-mail unless such data is found to be in violation of the HIPAA Policies and Procedures.

Protection of Information

8. Users of the e-mail system must ensure that all PHI forwarded, distributed, or printed is protected according to the HIPAA Policies and Procedures. Electronic PHI may be sent in an e-mail and/or over the internet provided it is adequately protected. To protect the integrity and privacy of ePHI transmitted electronically (i.e., via e-mail), the Health Plan shall:

    a. implement measures to ensure such ePHI is not improperly modified without detection by using network communications protocols, data or message authentication codes, or some similar measure; and

    b. implement encryption software and send ePHI in encrypted format in the following situations: [*insert situations in which risk analysis shows a significant risk that transmitted ePHI will be accessed by unauthorized entities*].

Responding to E-mail Messages

9. When an e-mail message is received containing PHI, any reply or response to that message (i.e., an acknowledgement or receipt of the message) must not include PHI. E-mail systems often automatically include the sender's e-mail message when a reply is made. When the original message includes PHI, the function of the software must be disabled or the original message must be manually deleted prior to sending a reply.

Maintaining/Archiving E-Mail Messages

10. E-mail messages may not be maintained or archived for more than thirty (30) days, unless otherwise approved by the HIPAA Privacy Officer.

Record Retention

11. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

12. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

13. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

14. Violations of this policy will be subject to discipline.

Effective Date

15. July 1, 2014.

References:

See generally 45 C.F.R. § 164.530, 45 C.F.R. § 164.312

Facsimile Machines

Policy Statement

The Health Plan utilizes facsimile (fax) machines to transmit data from one location to another on a routine basis. The Health Plan will provide physical and procedural safeguards to minimize the possibility of unauthorized observation or access to protected health information (PHI) during the transmission or receipt of data via a facsimile machine. This policy outlines the required elements for a secure location of a facsimile machine. The procedure establishes guidelines for how the Health Plan will reasonably safeguard the transmission and receipt of PHI via a facsimile machine to limit incidental or accidental use or disclosure of PHI.

Policy Interpretation and Implementation

Secure Location

1. Fax machines used to transmit or receive PHI shall be placed in secure locations. Whenever possible, fax machines used to receive PHI will not be used regularly for other purposes.

Pre-Programmed Numbers

2. Frequently used destination numbers will be pre-programmed into fax machines and tested before being used to transmit PHI. Each fax machine will display a key that identifies the destination for each pre-programmed fax number.

Non Pre-Programmed Numbers

3. When PHI is faxed to a destination number that is not pre-programmed, the fax machine operator will double-check the accuracy of the number in the machine's display before sending the fax.

Cover Letter

4. All fax messages will include a standard cover sheet, developed by the Privacy Officer, with the following (or substantially similar) statement:

   Confidentiality Statement: The documents accompanying this transmission contain confidential health information that is legally privileged. This information is intended only for the use of the individuals or entities listed above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

Transmittal Sheets

5. Transmittal sheets will be checked immediately after each transmission of PHI, to assure that the information was sent to the correct number.

Misdirected Faxes

6. If PHI has been sent to the wrong fax number, the sender must immediately send a second fax to the

number that was contacted in error, reiterating the confidentiality message, and asking the recipient to telephone the sender immediately to arrange proper disposition of the information. Any instance of transmitting PHI to the wrong destination number must be reported to the Privacy Officer immediately. The report must include the date, time, the wrong number, the correct number, the intended recipient, the identity of the member, and a brief description of the information that was transmitted in error. Transmission of PHI by fax to a wrong number must be included in an accounting of disclosures of PHI.

Received Faxes

7. Prior to distribution of a received fax message, the fax message must be reviewed to make sure that all pages that belong to that fax message have been received and are together, and pages that belong to other fax messages are not included. The cover sheet received with the message, if any, will be placed on top of the message.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

9. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

10. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

11. Violations of this policy will be subject to discipline.

Effective Date 12. July 1, 2014.

References:
See generally 45 C.F.R. § 164.530

Copy Machines

Policy Statement

The Health Plan utilizes copy machines to copy data on a routine basis. The Health Plan also occasionally utilizes third party copy services to copy data. The Health Plan will provide physical and procedural safeguards to minimize the possibility of unauthorized observation or access to protected health information (PHI) during the copying of data. This policy outlines the required elements for a secure location of a copy machine and establishes guidelines for how the Health Plan will reasonably safeguard PHI during copying to limit incidental or accidental use or disclosure of PHI.

Policy Interpretation and Implementation

Secure Location

1. Copy machines used to copy PHI shall be placed in secure locations. Whenever possible, copy machines used to copy PHI will not be used regularly for other purposes.

Removal of Original

2. Following the copying of any document containing PHI, the person making the copies will double-check to confirm that no original documents containing PHI are left on or at the copy machine.

Removal of Copies

3. Following the copying of any document containing PHI, the person making the copies will double-check to confirm that none of the copies containing PHI are left on or at the copy machine.

Erasing Memory

4. If the copy machine is equipped with a memory that allows the reprinting of a document previously copied, upon completion of the copy job involving documents containing PHI, the person making the copies will delete the memory and double-check that the memory has been deleted prior to leaving the copy machine.

Destruction of Certain Copies

5. In the event a copy containing PHI is unusable (because it is not dark enough, etc.) and is to be destroyed, the person making the copy will destroy the copy, regardless of whether it is legible, by shredding it.

Unattended Copying

6. In no instance shall the person making copies of documents containing PHI leave the copier unattended while copies are being made.

Outsourcing

7. To the extent possible, copies of PHI should be made on site in accordance with the foregoing procedures. In some instances it may, however, be appropriate to outsource copying of documents and data containing PHI to a third party copy service (i.e., large volumes of documents to copy or large numbers of copies needed). Prior to providing

documents/data containing PHI to any such copy service for copying, the copy service must sign a business associate agreement. Furthermore, the Mail policy shall be followed with respect to delivering the original documents/data to the copy service.

Record Retention

8. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

9. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

10. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

11. Violations of this policy will be subject to discipline.

Effective Date

12. July 1, 2014.

References:

See generally 45 C.F.R. § 164.530

Mail – Internal and External

Policy Statement

The Health Plan utilizes both internal and external mail (i.e., postal service and delivery services) to deliver data on a routine basis. The Health Plan will provide physical and procedural safeguards to minimize the possibility of unauthorized observation or access to protected health information (PHI) during the mailing of data. This procedure establishes guidelines for how the Health Plan will reasonably safeguard PHI during mailing of data to limit incidental or accidental use or disclosure of PHI.

Policy Interpretation and Implementation

Addresses

1. When PHI is mailed, whether internally or externally, the person sending the mail will double-check the accuracy of the address of the addressee before sending the mail.

Information Contained on Envelopes

2. When PHI is mailed, whether internally or externally, no PHI shall be included on the envelope, nor shall it be visible through the envelope, including any window in the envelope. With respect to internal mail, only the recipients name shall be indicated on the envelope.

Secure Envelopes

3. When PHI is mailed, whether internally or externally, it should be mailed in a sealed envelope or an envelope that may be securely closed and it should not be provided to unauthorized staff or third persons (i.e., mail room staff) until properly sealed or closed. To the extent it is impractical to place it in a secure envelope, interoffice mail may be transmitted without an envelope, provided that the first page of the mail does not contain PHI (i.e., a cover page is used or the first page is turned over) and PHI is not otherwise visible.

Receipt of Mail

4. Only authorized staff shall open mail that is received, whether from internal or external sources, from a subject of PHI or from any other party where it is likely the mail contains PHI. To the extent mail is received in an envelope that is not addressed to a specific person, where it is unclear that it is from the subject of PHI, or where it is unclear whether it may contain PHI, the mail may be opened by unauthorized staff, provided that person opening the envelope reviews the least amount of contents needed to determine to whom the mail is addressed and/or that it contains PHI, at which time the mail should be delivered to the appropriate person.

Record Retention

5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

6. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

7. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

8. Violations of this policy will be subject to discipline.

Effective Date

9. July 1, 2014.

References:
See generally 45 C.F.R. § 164.530

Storage of Documents

Policy Statement

Documents containing protected health information (PHI) will be stored so that they are protected from public view, view by those without a need to know whether inadvertent or otherwise, or unauthorized access.

Policy Interpretation and Implementation

Storage of Documents

1. Documents containing PHI shall be stored in locked file cabinets separate from other documents (i.e., personnel files) to which unauthorized staff may appropriately have access. Insofar as practical/feasible, the file cabinets shall be located in a secure location.

Access Limitations

2. Only authorized staff are granted access to individual and Health Plan information. Such access is limited to specific, denied, documented and approved applications and level of access rights.

Leaving File Cabinet Unlocked and Unattended

3. Authorized staff may not leave file cabinets containing documents with PHI unlocked and unattended for long periods of time (e.g., breaks, lunch, meetings, etc.). File cabinets must be locked at the end of the work shift.

Sharing Key to File Cabinet

4. Authorized staff may not (1) provide the key the any file cabinet containing PHI documents to other staff members or other non-staff members, or (2) allow other staff members or other non-staff members access to said file cabinets.

Record Retention

5. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

6. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

7. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be

directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

8. Violations of this policy will be subject to discipline.

Effective Date

9. July 1, 2014.

References:

See generally 45 C.F.R. § 164.530

Breach Notification Obligation

[HIPAA Privacy and Security]

Policy Statement

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), requires the Health Plan (i.e., a covered entity under HIPAA) to notify impacted individuals of a breach of their unsecured PHI. The purpose of this Breach Notification Obligation Policy is to establish guidelines for the Health Plan to satisfy its breach notification obligation.

Note: This Policy works in independently from other policies and procedures the Health Plan may have adopted to satisfy the HIPAA Privacy Rule. This Policy does not replace such policies and procedures.

Policy Interpretation and Implementation

Definition of Breach

1. For purposes of this Policy, a "breach" occurs when there is an acquisition, access, use, or disclosure of "unsecured" PHI in violation of the HIPAA Privacy Rule that compromises the security or privacy of the PHI.

"Unsecured" PHI

2. "Unsecured" PHI is the only PHI addressed under this Policy. Whether PHI is "unsecured" depends on the format in which the PHI exists; it does not depend on the type of PHI or the potential for harm if the PHI is breached. Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary. The Secretary recognizes two methods: (1) encryption in accordance with standards developed by the National Institute of Standards and Technology (NIST), and (2) destruction. Any other methods are considered unsecured.

Assessment

3. When a violation of the HIPAA Privacy Rule is discovered as described below, the Privacy Officer shall determine, based upon the factors identified below, the probability that the security or privacy of the PHI has been compromised.

   Note: There is a presumption that violations of the HIPAA privacy rule result in the compromise of the security or privacy of PHI. However, a breach occurs only if, based upon the assessment, the Privacy Officer determines there is a low probability that the security or privacy of the PHI has been compromised.

Discovery

4. Discovery by the Health Plan occurs when the 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 member of the Health Plan's workforce or its agent. See the "Third Party Assistance" section below for information regarding the status of third parties as agents of the Health Plan.

Relevant Factors

5. The determination of whether the violation compromises the security or privacy of the PHI is based upon the following four factors: (1) the nature and extent of the PHI involved (including, but not limited to, the types of identifiers included and the likelihood that the PHI may be re-identified); (2) the identity of the unauthorized user or recipient; (3) whether the PHI was actually acquired or viewed by the unauthorized user or recipient; or (4) the extent to which the risk to the PHI has been mitigated.

Documentation

6. The Health Plan shall document the assessment and keep such documentation with the Health Plan records in accordance to the record retention practices of the Health Plan.

Exceptions to this Policy

7. There are several specific exceptions to the application of this Policy. These are situations in which, absent the exception, there would be a breach requiring notification. A breach does not trigger the notification obligation if it consists of:

   (1) an unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of the Health Plan or its business associate, which was made in good faith and within the scope of the individual's authority, and which does not result in further impermissible uses or disclosures;

   (2) An inadvertent disclosure by an authorized person at the Health Plan to another authorized person at the Health Plan, which does not result in further impermissible uses or disclosures; and

   (3) a disclosure with respect to which the Health Plan has a good faith belief that the unauthorized person to whom PHI was disclosed would not reasonably be able to retain the information.

Notification Obligations

8. The details of the notification obligation (e.g., whom how, etc.) depend upon the number of individuals impacted and the nature of the breach.

Individual Notification

9. The Health Plan must notify the individuals whose PHI was the subject of the breach. Notification must be provided without reasonable delay, no later than sixty (60) calendar days after discovery by the Health Plan of the violation of the HIPAA Privacy Rule where such violation is subsequently determined by the Health Plan to be a breach.

   The notification should be in writing, mailed first class to the individual's last known address, unless the individual agrees to an electronic notification. The notification must include (1) a description of what happened; (2) a

description of the types of unsecured PHI involved; (3) the steps individuals should take to protect themselves; (4) a description of what is being done to investigate, mitigate, and protect from repeat occurrences in future; and (5) contact information for people with questions.

HHS Notification

10. The Health Plan must notify the Department of Health and Human Services (HHS) when a breach occurs. If the breach involves 500 or more individuals, the notification must take place coincident with the notification to the individuals. If the breach involves less than 500 individuals, immediate notification is not required. Notification for all breaches that occur within a calendar year must be made within sixty (60) days following the end of the calendar year.

Media Notification

11. Where the breach involves more than 500 residents of any one state or jurisdiction, the Health Plan must notify "a prominent media outlet" serving the state or jurisdiction. The notification must include the same information provided to the individuals and must take place within the same time frame as notification of the individuals.

Third Party Assistance

12. The Health Plan may contract with a third party for assistance in performing any or all of these functions. Unless specifically agreed to in writing, such third party will not be the Health Plan's agent.

HIPAA Privacy Officer

13. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

14. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

15. Violations of this policy will be subject to discipline.

Effective Date 16. July 1, 2014.

References:
Section 13402 of ARRA; 45 C.F.R. §§ 164.402 - .414.

Telecommuting

Policy Statement

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), requires the Health Plan (i.e., a covered entity under HIPAA) to implement policies and procedures to safeguard protected health information (PHI), including electronic protected health information (ePHI), maintained in connection with the Health Plan. These policies and procedures apply (1) both on and off the premises of the Health Plan, (2) while working from home or from another off-site location, and (3) regardless of whether such access is one-time situation, periodic, occasional or regular.

Policy Interpretation and Implementation

Application of Policies

1. This policy applies to all to situations in which a member of the Health Plan's workforce uses or accesses PHI remotely ("telecommutes") while off premises.

Workforce Members Must Sign Acknowledgement

2. A person permitted to telecommute must sign a document acknowledging that he or she:

    a. has completed any Employer-required privacy and security training, including those relating to HIPAA and the HITECH Act;

    b. has read and is familiar with the Employer's policies and procedures relating to confidentiality of information and access to Employer information systems;

    c. shall comply with all policies and procedures of the Employer relating to confidentiality of information and access to Employer information systems;

    d. shall keep any PHI, any Employer-owned equipment, and any devices or media (portable or otherwise, owned by the individual or by the Employer) on which PHI can be stored or accessed, in a secure location that is free from physical access by other individuals;

    e. shall not, while signed on, leave a secured computer application unattended;

    f. shall dispose of any work-related documents at a time and in a manner consistent with HIPAA and the HITECH Act and the Employer's requirements (e.g., by shredding paper documents and erasing or physically destroying electronic media containing PHI);

    g. shall not disclose any passwords or other sign-on information to anyone or allow anyone to access the Employer's systems or equipment using her or her sign-on information or password, and shall not attempt to access any Employer systems or equipment using sign-on information or passwords other than his or her own;

    h. shall, upon having reason to suspect that the

confidentiality of his or her user sign-on information or password has been compromised, immediately notify [responsible party] by calling the helpdesk at [Employer helpdesk phone number].

i. shall access, use, and disclose PHI only for job-related purposes in accordance with the requirements of HIPAA and the HITECH Act the Employer's privacy and security policy and procedures;

j. shall not save or store any PHI on his or her computer or on any portable electronic device or storage media (e.g., compact disk, flash drive, etc.) except as may be specifically authorized by the Employer in accordance with HIPAA and the HITECH Act and the Employer's privacy and security policy and procedures;

k. shall not transmit any PHI (to the Employer or otherwise) except in an encrypted format or through a secure line (e.g., using a VPN) in accordance with HIPAA, the HITECH Act, and the Employer's privacy and security policy and procedures;

l. shall not, except as otherwise explicitly allowed by the Employer's information security policy and privacy and security policies and procedures, use any Employer-owned equipment for personal use or install or use any programs on Employer-owned equipment other than as may be approved by the Employer;

m. shall install, update and use all antivirus software directed by the Employer in accordance with the Employer's requirements, and shall not disable, tamper with, or otherwise interfere with any Employer-provided antivirus software;

n. shall immediately notify [responsible party] upon discovery of any programs or devices (such as viruses, worms, Trojan horses, or other forms of malicious or potentially destructive computer code or computer sabotage) that could disrupt use of the Employer's information system or any system, equipment, or software to which such system is interfaced or connected, or could destroy, alter, damage, make inaccessible, or permit unauthorized access to any PHI;

o. shall immediately notify [responsible party] in the event that he or she has reason to suspect any unauthorized acquisition, access, use, or disclosure of PHI or any other potential security incident, and thereafter shall cooperate fully with any related investigation and mitigation actions;

p. shall comply with all laws that apply to him or her or to the Employer, including but not limited to HIPAA and the HITECH Act, and shall not act or fail to act

in a manner that would cause the Employer to fail to be in compliance with any law;

q. understands and agrees that use of the Employer's systems and equipment may be monitored periodically to ensure compliance with these provisions; and

r. understands and agrees that these obligations continue indefinitely and do not terminate even after termination of the individual's employment or other business relationship with the Employer.

Record Retention

3. A copy of all HIPAA covered information and any revisions shall be maintained for a period of at least six (6) years. Such retention may be in printed or electronic format, or both.

HIPAA Privacy Officer

4. The HIPAA Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the privacy of PHI. The HIPAA Privacy Officer is the contact person for any questions or complaints regarding HIPAA privacy. Questions or concerns about HIPAA rights should be directed to the HIPAA Privacy Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1051.

HIPAA Security Officer

5. The HIPAA Security Officer is responsible for the development and implementation of the HIPAA policies and procedures relating to the security of ePHI. The HIPAA Security Officer is the contact person for any questions or complaints regarding HIPAA security. Questions or concerns about HIPAA rights should be directed to the HIPAA Security Officer during regular business office hours Monday through Friday, except holidays at 218-894-2439 x1035.

Violations

6. Violations of this policy will be subject to discipline.

Effective Date

7. July 1, 2014.