HIPAA PRIVACY POLICIES AND PROCEDURES

LAKE ERIE REGIONAL COUNCIL'S GROUP HEALTH PLAN

Introduction

The Health Insurance Portability and Accountability Act of 1996, as amended, with pertinent overlay of the Health Information Technology for Economic and Clinical Health Act of 2009, and their implementing regulations (hereinafter "HIPAA"), restrict Covered Entities' and their Business Associates' Use and Disclosure of Protected Health Information ("PHI").

Lake Erie Regional Council's group health plan ("Health Plan") is a joint self-insurance program of Ohio public school districts and a Covered Entity. All of Health Plan's Workforce are employees of Health Plan, Plan Sponsor, and/or Plan Sponsor's member school districts (individually, a "Member" or collectively, the "Members").

It is the policy of Health Plan to comply fully with HIPAA and all employees of the Members who have access to PHI about Health Plan's participants must comply with these HIPAA Privacy Policies and Procedures (these "Policies and Procedures"), as evidenced by a signed employee confidentiality agreement.

These Policies and Procedures address HIPAA, not other federal or state laws. These Policies and Procedures shall be interpreted to comply with HIPAA to the extent applicable. To the extent these Policies and Procedures establish requirements and obligations above and beyond those required by HIPAA, they shall be aspirational and non-binding.

No third party rights (including, but not limited to, rights of Health Plan participants, beneficiaries, covered dependents, or Business Associates) shall be created by these Policies and Procedures.

These Policies and Procedures are effective as of September 23, 2013.

Health Plan reserves the right to amend or change these Policies and Procedures at any time (and even retroactively) without notice.

HIPAA Privacy Policies and Procedures

Table of Contents

DEFINITIONS

Unless otherwise provided, the following definitions shall be used in the interpretation of these Policies and Procedures. For additional HIPAA capitalized terms not defined below, see 45 *Code of Federal Regulations* Parts 160 and 164.

Breach means the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the Privacy Rules, which compromises the security or privacy of the PHI. Breach excludes:

- Any unintentional acquisition, access, or Use of PHI by a Workforce member or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access, or Use was made in good-faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted by the Privacy Rules.

- Any inadvertent Disclosure by a person authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement in which Health Plan participates, and the information received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted by the Privacy Rules.

- A Disclosure of PHI where a Covered Entity or Business Associate has a good-faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

Business Associate means a person or organization who on behalf of Health Plan, but other than in the capacity of a member of the Workforce, creates, receives, maintains or transmits PHI for a function or activity regulated by the Privacy Rules, including claims processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR §3.20, billing, benefit management, practice management and re-pricing; or who provides, other than in the capacity of a member of the Workforce, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for Health Plan where the provision of the service involves the Disclosure of PHI from Health Plan or from another Business Associate of Health Plan to the person.

Covered Entity means a health plan, health care clearinghouse, or health care provider.

Designated Record Set means any item, collection, or grouping of information that includes PHI, maintained by or for Health Plan, in an enrollment, Payment, claims adjudication, or case or medical management record system; or, that is used, in whole or part, by or for Health Plan to make decisions about Individuals.

Disclosure is any release, transfer, provision of access to, or divulging in any other manner of PHI to persons outside Health Plan.

Electronic PHI ("ePHI") means PHI (i) maintained in Electronic Media (electronic storage material on which data is or may be recorded electronically) for example, computer memory devices (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card, or (ii) transmitted by Electronic Media (transmission media used to exchange information already in electronic storage media) for example, the Internet, extranet or intranet, phone lines, and networks. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via Electronic Media if the information being exchanged did not exist in electronic form immediately before the transmission.

Genetic Information means, with respect to any Individual, information about (i) such Individual's genetic tests, (ii) the genetic tests of family members of such Individual, (iii) the manifestation of a disease or disorder in family members of such Individual, or (iv) any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the Individual or any family member of the Individual.

Health Care Operations means any of the following activities to the extent that they are related to plan administration: conducting quality assessment and improvement activities; reviewing health care professionals or Health Plan performance; underwriting and premium rating; conducting or arranging for medical review, legal services and auditing functions; business planning and development; and business management and general administrative activities.

HHS means the United States Department of Health and Human Services.

Individual means the person ("patient") who is the subject of the PHI at issue and shall have the meaning set forth in 45 CFR §160.103, and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

Minimum Necessary means (when Using, Disclosing, or requesting PHI) making reasonable efforts to limit the Use or Disclosure of PHI to that minimally necessary to accomplish the intended purpose of the Use, Disclosure or request.

Payment means activities undertaken to obtain premiums or to determine or fulfill Health Plan's responsibility for coverage and provision of benefits under the plan, or to obtain or provide reimbursement for health care, that relate to an Individual to whom health care is provided and include, but are not limited to: eligibility and coverage determinations (including coordination of benefits); adjudication or subrogation of health benefit claims; risk adjusting based on enrollee status and demographic characteristics; billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance), and related health care data processing; medical necessity reviews; utilization reviews; and Disclosure to consumer reporting agencies of any Individual's name, address, DOB, SSN, payment history, account number, and name and address of Health Plan.

Plan Administration Functions means administration functions performed by a Plan Sponsor on behalf of Health Plan and excludes functions performed in connection with any other benefit or benefit plan.

Plan Sponsor means the Lake Erie Regional Council.

Privacy Rules means Subpart E of the Health Insurance Portability and Accountability Act (45 CFR §§164.500 – 164.534).

Protected Health Information ("PHI") is information, transmitted or maintained in any form or medium, created or received by Covered Entities that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future Payment for the provision of health care to an Individual; and that identifies an Individual or for which there is a reasonable basis to believe the information can be used to identify an Individual. Protected Health Information includes information regarding persons living or deceased (up to 50 years post death).

Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable through encryption, destruction or other approved methodologies.

Use is the sharing, employment, application, utilization, examination, or analysis of PHI by any person working within Health Plan.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Health Plan, is under the direct control of Health Plan or a Member.

POLICIES AND PROCEDURES

POLICY

Health Plan shall implement policies and procedures with respect to PHI reasonably designed to comply with the Privacy Rules and Breach notification requirements and to ensure Workforce compliance. These Policies and Procedures shall be amended as necessary and appropriate to comply with changes in the law or changes in Health Plan's privacy practices. Any such amendments shall be promptly documented and implemented and notice given if appropriate.

PROCEDURE

These Policies and Procedures should be reviewed as necessary and periodically, at least once every two years, to determine changes necessary and appropriate to comply with the Privacy Rules and Breach notification requirements.

Any changes to these Policies and Procedures should be reasonably designed to ensure compliance, taking into account the size and type of PHI activities undertaken by Health Plan.

If a change in law or Health Plan's privacy practices impacts Health Plan's Notice of Privacy Practices, it may need to be promptly revised and redistributed to all of Health Plan's participants. The Privacy Officer should work with legal counsel for Health Plan to determine if any change is material and whether the change may be effective with respect to PHI created or received before the effective date of notice.

REFERENCES/CITATIONS
45 CFR §164.530(i)

PERSONNEL DESIGNATIONS

POLICY

Health Plan shall designate a Privacy Officer to assume responsibility for developing and implementing these Policies and Procedures. The Privacy Officer shall also be designated the contact person responsible for receiving complaints and to provide further information about matters covered by Health Plan's Notice of Privacy Practices. Health Plan shall update and maintain documentation of these personnel designations.

PROCEDURE

Health Plan may require certain qualifications of its Privacy Officer (e.g. education, knowledge of information privacy laws, or organization, facilitation, communication, and presentation skills).

The Privacy Officer should perform the following duties, as appropriate:

- Update and distribute Health Plan's Notice of Privacy Practices;
- Perform a periodic risk assessment of policies, procedures, and responsible personnel; and determine timeframes and resources necessary to address any gaps;
- Work with legal counsel, management, and departments to ensure Health Plan has, and maintains, sufficient privacy practices;
- Review and update these Policies and Procedures as appropriate;
- Document that required training occurs in a timely manner;
- Facilitate activities to foster information privacy awareness within Health Plan;
- Inform Workforce members when privacy practices are changed or updated;
- Oversee rights to inspect and amend PHI as appropriate, and restrict access to PHI when appropriate;
- Receive, document, track, investigate, and take action on all complaints concerning these Policies and Procedures, Health Plan's compliance therewith or with any other HIPAA requirement;
- Implement corrective action to mitigate effects of inappropriate Use or Disclosure of PHI and document such actions;

- Identify Business Associates that receive PHI and, in collaboration with legal counsel, review existing contracts with these parties for compliance with HIPAA;

- Take proper discovery and notice steps on report of any Breach of Unsecured PHI; and

- Cooperate with HHS and Health Plan's Members in any and all compliance reviews or investigations.

REFERENCES/CITATIONS
Privacy Officer: 45 CFR §164.530(a)(1)(i)
Contact Person: 45 CFR §§164.520(b)(1)(vii), 164.524(d)(2)(iii), 164.526(d)(1)(iv), 164.530(a)(1)(ii)

MINIMUM NECESSARY

POLICY

When Using, Disclosing or requesting PHI, Health Plan shall make reasonable efforts to limit PHI to the Minimum Necessary to accomplish the intended purpose of the Use, Disclosure or request.

PROCEDURE

This Minimum Necessary policy does not apply to:

Disclosures to or requests by a health care provider for Treatment;
Uses or Disclosures to the Individual or their personal representative;
Uses or Disclosures made pursuant to an authorization;
Disclosures to the Secretary of HHS;
Uses or Disclosures required by law; or
Uses or Disclosures required for compliance with the Privacy Rules.

All other types of Uses, Disclosures or requests, if any, should be reviewed as necessary or appropriate on an individual basis with Privacy Officer to ensure the Minimum Necessary to accomplish its purpose.

Disclosures of PHI to Plan Sponsor should be limited to the performance of Plan Administration Functions. (See Plan Sponsor/Adequate Separation Policy and Procedure.)

To the extent practicable, Health Plan should Use, Disclose, or request de-identified health information. (See De-identification of PHI Policy and Procedure.)

In most cases the health-related information held by Health Plan is limited to enrollment data. In limited instances it may also include information that participants of Health Plan provided to certain Workforce members and/or Business Associates to assist with the coordination of Individual benefits or claims. Medical and claims information is maintained by Business Associates of Health Plan.

When requesting PHI, Workforce members should limit the amount requested to that reasonably necessary to accomplish the purpose of the request. Workforce members should never request PHI in an electronic format. (See No Electronic PHI Policy and Procedure.)

When Disclosing PHI, Workforce members should limit the amount Disclosed to that reasonably necessary to accomplish the purpose for which Disclosure was requested. Effort should also be made to obtain written representation from the party seeking Disclosure that the requested PHI is the Minimum Necessary for the stated purpose.

Each Member must identify appropriate Workforce members who need access to PHI to carry out their duties; and, for each such person, the categories of PHI needed and any conditions

appropriate to such access. Reasonable effort should be made to so limit such access. (See Workforce Policies and Procedure.)

For routine or recurring requests or Disclosures, Health Plan should limit PHI to that reasonably necessary and may periodically review, on an individual basis, such requests or Disclosures. Each Workforce member is responsible for determining what is necessary to accomplish the intended purpose of a PHI Use, Disclosure or request.

Health Plan may reasonably rely on a Disclosure request, as the Minimum Necessary for the stated purpose, when:

1. Public officials so represent;
2. The information is requested by another Covered Entity; or
3. Workforce members, Business Associates or research organizations provide written representations.

Health Plan should never Use, Disclose or request an entire medical record, except when specifically justified as the amount that is reasonably necessary to accomplish the intended purpose.

REFERENCES/CITATIONS
45 CFR §§164.502(b), 164.514(d), (e)(2)

NO ELECTRONIC PHI

POLICY

It is the policy of Health Plan **not** to create, receive, maintain or transmit ePHI.

PROCEDURE

For recurring processes, Health Plan may access ePHI through the secure information systems of its Business Associates but shall limit such access to the reasonably minimum amount required. No ePHI may be downloaded from such systems. Information may be printed directly from such systems but such print copies must be maintained and stored in accordance with these Policies and Procedures.

Members may periodically review information systems activity records, including audit logs, access reports, and security incident tracking reports to ensure that there is no unauthorized access to ePHI.

PHI should never be scanned into electronic format.

PHI should never be transmitted by e-mail, but rather, by mail or facsimile.

Despite Health Plan's best efforts, should any Workforce member incidentally encounter ePHI, he or she should securely destroy or delete the ePHI immediately.

REFERENCES/CITATIONS
45 CFR §160.103

DE-IDENTIFICATION OF PHI

POLICY

Whenever reasonably possible, de-identified information should be used, rendering PHI anonymous by way of completely removing identifying characteristics.

PROCEDURE

Health Plan may freely Use and Disclose de-identified information. There are two ways that information can be de-identified: either by professional statistical analysis or by removal of 17 specific identifiers plus any other unique identifying number, characteristic or code.

De-identified information is Health Information that does not identify an Individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an Individual.

Workforce members can de-identify PHI through the elimination of primary or obvious identifiers (name, address, date of birth) and secondary identifiers (through which a user could deduce an Individual's identity). All the following information about the Individual, his or her relatives, employers and household members must be removed:

1. names;
2. geographic information smaller than a state (street address, city, county, zip code);
3. dates related to the Individual (birth, age, admission, discharge, death);
4. phone numbers;
5. fax numbers;
6. email addresses;
7. social security numbers (SSNs);
8. medical record numbers;
9. health beneficiary plan numbers;
10. account numbers;
11. certificate/license numbers;
12. VINs and license plates;
13. Device IDs and serial numbers;
14. URLs and IP addresses;
15. Finger and voice prints;
16. Images; and
17. any other unique identifying number characteristic, or code.

Health Plan may Use PHI to create de-identified information, or may Disclose PHI to a Business Associate for such purpose, whether or not the de-identified information will be used by Health Plan.

If de-identified information is re-identified it becomes subject to the Privacy Rules again and may only be Used or Disclosed in compliance with the Privacy Rules and these Policies and Procedures.

Workforce members must consult with Privacy Officer prior to Disclosure when concerned about or relying on the status of information as de-identified.

De-identified health information is not PHI and therefore is exempt from the Policies and Procedures entitled Access to Inspect and Copy PHI, Requests for Amendment, and Accounting of PHI Disclosures.

REFERENCES/CITATIONS
45 CFR §164.514(a), (b), (c)

VERIFICATION

POLICY

Except with respect to Disclosures for notice of or involvement in an Individual's care, Health Plan, prior to Disclosing PHI, shall verify the identity of a person requesting PHI, and his or her authority to do so if not known, and shall obtain any required documents or representations from the requestor upon which the Disclosure is conditioned.

PROCEDURE

Workforce members may rely, if reasonable under the circumstances, on documentation, statements or representations that, on their face, meet applicable requirements.

To verify the authority of a public official or a person acting on their behalf, Workforce members may rely, if reasonable under the circumstances, on agency ID badge, official credentials, proof of government status, appropriate letterhead, or other good evidence.

Appropriate proof of authority on behalf of the Individual may include, without limitation and as reasonable for the situation, identification as parent, guardian, or executor, power of attorney, or other evidence of appropriate relationship with the Individual, a warrant, subpoena, order or other legal process issued by a grand jury, a court or administrative tribunal, or a written statement of legal authority.

Workforce members should exercise professional judgment and act in good-faith with respect to verification requirements.

If any Workforce member has doubt or question about whether sufficient verification has been obtained, Privacy Officer must be consulted before Disclosure.

Workforce members should document and maintain information relied upon, including any oral representations.

REFERENCES/CITATIONS
45 CFR § 164.514(h)

DECEASED INDIVIDUALS

POLICY

Health Plan shall ensure that the PHI of deceased Individuals is subject to the same standards regarding Use and Disclosure as apply to the PHI of living Individuals.

PROCEDURE

These Policies and Procedures remain in effect for a period of fifty (50) years following the death of an Individual.

Except with respect to organ donation, coroners, medical examiners, and funeral directors (see Uses and Disclosures: Authorization Not Required Policy and Procedure), Workforce members must not release PHI regarding a deceased Individual unless a valid personal representative has been established.

Workforce members must document and maintain information relied upon, including any oral representations.

REFERENCES/CITATIONS
45 CFR§§164.502(f), (g)(4), 164.512(g)

PERSONAL REPRESENTATIVES

POLICY

Health Plan shall treat a person as the personal representative of an Individual if the person is, under applicable state or other law, authorized to act on behalf of the Individual in making decisions related to health care.

PROCEDURE

Personal representative may include parents, legal guardians or properly appointed agents, like those identified in a Durable Power of Attorney for Health Care. Personal representative status documentation relied upon must be copied and maintained with the Individual's PHI.

Where appropriate personal representative status has been established, Workforce members should treat personal representatives as the Individual.

Workforce members must inform Privacy Officer whenever they believe it is not in the best interest of an Individual to treat a person as a personal representative.

REFERENCES/CITATIONS
See 45 CFR §164.502(g)

DOCUMENTATION

POLICY

Health Plan shall maintain, in written or electronic form, these Policies and Procedures, all HIPAA Privacy communications required to be in writing, and all HIPAA Privacy actions, activities or designations required to be documented. Required HIPAA documentation shall be retained by Health Plan for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

PROCEDURE

Workforce members shall keep separate from any other paperwork (for example, in a unique accordion file or cabinet/storage location) all written documentation of compliance with and implementation of the Privacy Rules.

Workforce members shall keep separate from any other electronic documents (for example, in a single folder or directory) all electronic documentation of compliance with and implementation of the Privacy Rules.

REFERENCES/CITATIONS
45 CFR §164.530(j)

SAFEGUARDS

POLICY

Health Plan shall put in place appropriate Administrative, Technical, and Physical Safeguards to protect the privacy of PHI.

PROCEDURE

The requirements of these Policies and Procedures for the Minimum Necessary, No ePHI and Verification together form the basis of Health Plan's efforts to safeguard PHI. In addition, the following safeguards shall be implemented and Health Plan may use any other reasonable and appropriate security measures. Reasonable safeguards implemented shall include consideration of intentional, unintentional and incidental Uses or Disclosures.

Privacy Officer may periodically assess and monitor Health Plan's compliance regarding its reasonable efforts to safeguard PHI. Privacy Officer may perform a periodic risk analysis to provide an assessment of potential risks/vulnerabilities to the confidentiality, integrity, and availability of PHI.

Additional training, discipline or other measures to ensure and/or improve compliance may be implemented when appropriate.

Only Workforce members who need access to PHI to perform their duties shall have access to PHI. Only those Workforce members shall have access to keys for locked areas, such as doors and filing cabinets, which contain PHI. Each Member shall ensure that all PHI is kept in areas with physical security controls that restrict access and no PHI shall be removed from the premises of such Member.

Only designated workstations shall be used to access PHI. These workstations shall not be located in publicly accessible areas or be used by multiple users unless all are authorized to access PHI. Each Workforce member using a designated workstation should have a separate log-in ID and password. Designated workstations should be set to auto log-out if not used within a reasonable period of time. ePHI shall not be accessed from any computer other than the designated workstations.

PHI received by a Workforce member shall be promptly placed in a locked area.

PHI on hard copy mediums approved for destruction by a Member must be shredded or otherwise made unreadable and unable to be reconstructed before disposal.

Any PHI received on or by electronic medium shall be promptly cleared, destroyed, or purged so that it cannot be reconstructed. A print copy of such PHI may be retained, if necessary.

Workforce members are encouraged to promptly report any violation of this policy to Privacy Officer. Any such reports may be made anonymously.

Workforce members must cooperate fully with any safeguards investigation, corrective action or sanction instituted by Privacy Officer.

REFERENCES/CITATIONS
45 CFR §§164.304, 164.530(c)

WORKFORCE

POLICY

All employees of Members who are part of the Workforce must comply with the Privacy Rules and these Policies and Procedures and are required to sign a confidentiality agreement for this purpose.

PROCEDURE

Only the following employees shall be Workforce members and have access to PHI:

employees who perform Plan Administration Functions on behalf of Health Plan; and

employees who receive PHI relating to Payment, Health Care Operations or other matters pertaining to Health Plan in the ordinary course of business.

Health Plan has identified these employees as the classes of persons who need access to PHI to carry out their duties. Each Member is responsible for determining, for its employees, the category or categories of PHI to which access is needed.

Reasonable effort must be made to limit the access of these employees to the category or categories of PHI needed to carry out their duties.

REFERENCES/CITATIONS
45 CFR §§160.103, 164.504(a), 164.514(d)

TRAINING

POLICY

All Workforce members shall receive training on these Policies and Procedures, as necessary and appropriate for them to carry out their Health Plan functions.

PROCEDURE

Within a reasonable period of time after the adoption, and any amendment, of these Policies and Procedures, Health Plan will train all members of the Workforce on these Policies and Procedures. New employees hired after the adoption of these Policies and Procedures must be trained within a reasonable period of time, before they perform work for Health Plan involving PHI. Any Workforce members whose job functions are affected by a material change to these Policies and Procedures should receive additional training within a reasonable period of time after the material change.

Workforce members are required to attend scheduled training.

Workforce members shall be provided a copy of these Policies and Procedures and shall review them as needed and at least once every year.

Workforce members shall be trained to recognize and promptly report HIPAA violations to Privacy Officer.

Training shall include notice that criminal penalties or restitution for the wrongful Disclosure of PHI are enforceable against Workforce members who knowingly and without authorization obtain or Disclose PHI.

Workforce members may be asked to sign an updated confidentiality agreement as a part of training; and may request additional training at any time.

Privacy Officer must evaluate the effectiveness of training and document all Workforce training on these Policies and Procedures.

REFERENCES/CITATIONS
45 CFR §§164.530(b), (j)

SANCTIONS

POLICY

Workforce members who fail to comply with these Policies and Procedures or the Privacy Rules or Breach notification requirements will be subject to appropriate sanctions imposed in accordance with the discipline policies of the Members with which they are employed, up to and including termination of employment. All sanctions applied, if any, shall be documented. Whistle-blowers shall not be sanctioned, provided they act reasonably and in good-faith.

PROCEDURES

If warranted, a Member should impose, in accordance with its local policies and agreements, discipline that is appropriate to the nature of the violation that prompted the disciplinary action. Discipline may include, but not be limited to, a fine, probation, suspension, additional training, and/or termination.

Each Member should ensure that the imposed discipline is adequately communicated to the violator and enforced.

Independent contractors are considered Health Plan's Business Associates, not Workforce members, and are not subject to discipline under these Policies and Procedures. For violations that originate outside Health Plan, Privacy Officer shall consult any applicable Business Associate Agreement to determine steps to cure, and whether termination may be necessary.

REFERENCES/CITATIONS
45 CFR §§164.502(j), 164.530(e), (g)(2)

COMPLAINTS

POLICY

Health Plan shall provide a process for Individuals to make complaints concerning these Policies and Procedures, or Health Plan's compliance with these Policies and Procedures, or Health Plan's compliance with the Privacy Rules or Breach notification requirements.

PROCEDURE

Any Individual wishing to complain to Health Plan shall be directed to the Privacy Officer.

Privacy Officer will accept any such complaint.

Individuals should be encouraged to submit complaints in writing, and to state in clear terms the nature of the complaint, and to provide any information necessary to enable Health Plan to investigate and review the complaint.

Individuals insisting on an oral complaint should be asked to explain their complaint in sufficient terms and Privacy Officer should document this input as best possible.

Privacy Officer shall maintain a log documenting all complaints received and their disposition, if any.

If any Individual asks how he or she may file a complaint with HHS, the Individual shall be directed to Health Plan's Notice of Privacy Practices.

Privacy Officer, or his or her designee, must investigate and handle as a quality-review matter all complaints submitted, as appropriate, interviewing or otherwise contacting other persons involved in the circumstances upon which the complaint is based, and take other steps necessary to review and investigate the complaint.

Any PHI received because of a complaint must be de-identified before further Use or Disclosure.

Privacy Officer shall provide the complaining Individual with written notice including: (a) the name of the individual handling the complaint; (b) the fact that an investigation has/will take place; (c) the date of completion or expected completion; and (d) due to the confidential and privileged nature of the quality-review process, the results of such proceedings may not be communicated to the Individual.

Following completion of an investigation, Privacy Officer may determine whether any of the following occurred: (a) Workforce member(s) failed to comply with these Policies and Procedures; (b) Workforce member(s) failed to comply with the Privacy Rules or Breach notification requirements; or (c) these Policies and Procedures failed to fully address the Privacy Rules or Breach notification requirements.

To the extent Privacy Officer determines any Workforce member failed to comply with these Policies and Procedures and/or HIPAA, Privacy Officer may recommend to the Member with which such Workforce member is employed that such Workforce member be disciplined.

To the extent Privacy Officer determines these Policies and Procedures failed to fully address the Privacy Rules or Breach notification requirements, he or she shall propose that they be amended promptly.

REFERENCES/CITATIONS

Business Associate: 45 CFR §160.306
Covered Entity: 45 CFR §§164.520(b)(vi) & 164.530(a), (b), (d), (g), (h)

NO INTIMIDATING OR RETALIATORY ACTS

POLICY

Workforce members shall not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against Individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

PROCEDURE

Discussion of this Health Plan restraint policy shall be highlighted in Workforce training.

REFERENCES/CITATIONS
45 CFR §§164.530(g), 160.316

NO WAIVER OF RIGHTS

POLICY

No Individual shall be required to waive his or her privacy rights under HIPAA as a condition of the provision of Treatment, Payment, enrollment in Health Plan or eligibility for benefits.

PROCEDURE

Discussion of this Health Plan restraint policy shall be highlighted in Workforce training.

REFERENCES/CITATIONS
45 CFR §§164.530(h), 160.306

USES AND DISCLOSURES:
GENERAL RULE

POLICY

Health Plan shall not Use or Disclose PHI except as permitted or required by HIPAA.

PROCEDURE

All Disclosure of PHI shall be centralized through Workforce members who have been properly trained in accordance with these Policies and Procedures.

See other Procedures under pertinent Polices set forth in these Policies and Procedures.

REFERENCES/CITATIONS
See 45 CFR §164.502(a)

USES AND DISCLOSURES:
GENETIC INFORMATION

POLICY

Health Plan shall not Use or Disclose PHI that is Genetic Information for underwriting purposes.

PROCEDURE

Workforce members shall be cautious that information relied upon to conduct any of the following activities does not contain any Genetic Information:

- Determining eligibility (including enrollment and continued eligibility)
- Determining benefits under Health Plan (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment)
- Computing premium or contribution amounts (including discounts, rebates, payments in kind, or other premium mechanisms in return for activities such as completing a health risk assessment).
- Creating, renewing or replacing a contract of health insurance or health benefits.

Health Plan's Notice of Privacy Practices contains a statement that Health Plan is prohibited from using or Disclosing PHI that is Genetic Information for underwriting purposes.

REFERENCES/CITATIONS
45 CFR §§160.103, 164.502(a)(5)(i), 164.520(b)(1)(iii)(C)

USES AND DISCLOSURES:
REQUIRED DISCLOSURES

POLICY

Health Plan shall Disclose PHI to an Individual, when requested under and required by HIPAA's Access to Inspect or Accounting for PHI Disclosures rules.

Health Plan shall Disclose PHI when required by the Secretary of HHS to investigate or determine Health Plan's compliance with HIPAA.

PROCEDURE

See the Procedures under pertinent Policies set forth in these Policies and Procedures.

REFERENCES/CITATIONS
See 45 CFR §§164.502(a)(2)

USES AND DISCLOSURES:
TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

POLICY

See Uses and Disclosures General Rule.

PROCEDURE

Health Plan may Use and Disclose PHI for Health Plan's own Payment or Health Care Operations.

> Workforce members that have any uncertainty about whether a task they may perform involving PHI constitutes a Payment or Health Care Operation shall promptly contact Privacy Officer.

Health Plan may Disclose PHI for Treatment activities of a health care provider.

Health Plan may Disclose PHI to another Covered Entity or health care provider for its Payment activities.

PHI may also be Disclosed to another Covered Entity for purposes of that Covered Entity's quality assessment and improvement, case management, health care fraud and abuse detection programs, review and evaluation of professionals, plan performance or for provider training, if the other Covered Entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

> NOTE – Uses and Disclosures of PHI for Treatment are not subject to the Minimum Necessary standard. Uses and Disclosures of PHI for Payment or Health Care Operations are subject to the Minimum Necessary standard.

Workforce members shall verify the identity and authority of recipients in all instances of Disclosure of PHI for Treatment, Payment or Health Care Operations.

REFERENCES/CITATIONS
45 CFR §§164.502, 164.504, 164.506, 164.514

USES AND DISCLOSURES:
AUTHORIZATION REQUIRED

POLICY

Health Plan shall not Use or Disclose Psychotherapy Notes without a valid authorization.
Health Plan shall not Use or Disclose PHI for Marketing without a valid authorization.
Health Plan shall not sell PHI without a valid authorization.

PROCEDURE

A valid authorization contains many required elements, some specific to the intended use. Further, Health Plan may in only very limited circumstances condition the provision of Treatment, Payment, enrollment or eligibility for benefits on the provision of an authorization.

Any contemplated Use or Disclosure of PHI for the above purposes shall be reviewed with Privacy Officer in advance.

REFERENCES/CITATIONS
See 45 CFR §164.508

USES AND DISCLOSURES:
FUNDRAISING

POLICY

HIPAA allows Health Plan to Disclose certain PHI to a Business Associate or an institutionally related foundation, without an authorization for fundraising purposes. However, it is the policy of Health Plan **not** to engage in fundraising activities.

PROCEDURE

Should Health Plan engage in fundraising activity, Health Plan will amend this Policy and its Notice of Privacy Practices to include a statement documenting its intentions to contact Individuals to raise funds and informing Individuals' of their right to opt-out of receiving such communications.

REFERENCES/CITATIONS
45 CFR §§164.514(f), 164.520(b)(1)(iii)

USES AND DISCLOSURES:
FOR NOTICE OF OR INVOLVEMENT IN AN INDIVIDUAL'S HEALTH CARE

POLICY

See Uses and Disclosures General Rule.

PROCEDURE

If a family member, relative or close personal friend contacts Health Plan seeking PHI about an Individual, a Workforce member shall first attempt to contact the Individual for his or her authorization.

If the Individual is not available or able to provide his or her agreement:

(a) Health Plan may Disclose to family members, relatives or close personal friends PHI directly relevant to such person's involvement with the Individual's health care or Payment; or

(b) Health Plan may Use or Disclose PHI to notify or assist in notifying (identify or locate) a family member, personal representative or other person responsible for the Individual's health care about the Individual's location, general condition or death.

It should reasonably be inferred from the circumstances and based on the exercise of professional judgment that the Individual would not object to the Disclosure.

Any such Use or Disclosure shall be made only when in the best interests of the Individual.

Only the Minimum Necessary amount of PHI shall be Disclosed.

REFERENCES/CITATIONS
See 45 CFR §§164.510(b)

USES AND DISCLOSURES:
AUTHORIZATION NOT REQUIRED

POLICY

See Uses and Disclosures General Rule.

PROCEDURE

In the following situations, Health Plan may Disclose PHI without an Individual's consent or authorization:

1. regarding victims of abuse, neglect or domestic violence;

Health Plan must reasonably believe the Individual is a victim and the Disclosure is necessary to prevent serious harm. Workforce members shall verify the authority of any requesting agency to receive such reports. Disclosure must comply with and be limited to the relevant legal requirements. Health Plan shall promptly inform the Individual of the Disclosure unless doing so would place the Individual at risk.

2. for judicial and administrative proceedings;

Disclosures in response to an order of a court/administrative tribunal must be limited to only the PHI expressly authorized by such order. Disclosures in response to a subpoena must be made only after a requestor has provided satisfactory assurance that it has notified the Individual who is the subject of the PHI or efforts have been made to secure a qualified protective order.

3. for law enforcement purposes;

The types and requirements of these Disclosures are multiple. Privacy Officer shall reference the applicable HIPAA standard (45 CFR §164.512(f)) to determine appropriate steps whenever such a request is made.

4. for public health activities;

The types and requirements of these Disclosures are multiple. Typical scenarios include: disease prevention, reporting of injuries or vital events, child abuse or neglect, FDA regulation, communicable diseases, medical surveillance, and immunization records. Privacy Officer shall reference the applicable HIPAA standard (45 CFR §164.512(b)) to determine appropriate steps when such a request is made.

5. for health oversight activities;

Such Disclosures must relate to oversight activities authorized by law or activities necessary for appropriate oversight of the health care system, or government benefit programs. Workforce members shall verify the authority of any requesting agency.

6. regarding an Individual who has died;

Disclosure may be made to a coroner or medical examiner for identification, cause of death determination, or other duties authorized by law. Disclosure may be made to funeral directors as necessary to carry out their duties with respect to the decedent.

7. for cadaveric organ, eye or tissue donation purposes;

Such Disclosures shall only be made for the purpose of facilitating donation or transplantation.

8. for research purposes;

These Disclosures shall be made only after Health Plan receives certain necessary professional approvals and researcher representations. Privacy Officer shall reference the applicable HIPAA standard (45 CFR §164.512(i)) to determine appropriate steps whenever such a request is made.

9. to avert a serious threat to health or safety;

Health Plan must have a good-faith belief that the Use or Disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Health Plan must also have a good-faith belief that the Use or Disclosure is to a person reasonably able to prevent or lessen the threat.

10. for specialized government functions; and

The types and requirements of these Disclosures are multiple. Typical scenarios include: military and veteran activities, national security and intelligence, and correctional institutions. Privacy Officer shall reference the applicable HIPAA standard (45 CFR §164.512(k)) to determine appropriate steps whenever such a request is made.

11. related to workers' compensation.

Workforce members shall verify the Disclosure is authorized by and necessary to comply with such laws.

REFERENCES/CITATIONS
45 CFR §164.512

USES AND DISCLOSURES:
PURSUANT TO AN AUTHORIZATION

POLICY

See Uses and Disclosures General Rule.

PROCEDURE

Except for Genetic Information for underwriting purposes, PHI may be Used or Disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by an Individual.

An authorization for Use or Disclosure of PHI form should be provided to any Individual on request.

Workforce members shall make sure authorization forms are filled-out completely.

All Uses and Disclosures made pursuant to a valid authorization must be consistent with the terms and conditions of the authorization.

To the extent not yet relied thereon, Health Plan shall honor any written request to revoke an authorization.

If Health Plan or a Member requests an authorization, the Individual must be provided a signed copy.

REFERENCES/CITATIONS
45 CFR § 164.508(a)(1), (b) and (c)

BUSINESS ASSOCIATE AGREEMENTS

POLICY

Health Plan shall enter into a contract with all Business Associates that establishes the permitted and required Uses and Disclosures of PHI by Business Associate, contains all HIPAA required provisions, and authorizes unilateral termination by Health Plan for violations. PHI shall not be Disclosed by Health Plan to any outside consultant or contractor until a Business Associate Agreement containing satisfactory assurances is fully executed.

PROCEDURE

Workforce members may Disclose PHI to Health Plan's Business Associates and allow Health Plan's Business Associates to create or receive PHI on Health Plan's behalf only once Health Plan has obtained written satisfactory assurances from its Business Associates that they will appropriately safeguard PHI.

If any Workforce member is unsure whether an outside consultant or contractor has entered into a Business Associate Agreement with Health Plan, the Workforce member must contact the Privacy Officer and verify that a Business Associate Agreement is in place.

Business Associates have a statutory obligation to comply with the terms of their Business Associate Agreements and HIPAA. Any questions about Business Associate PHI access, Use, Disclosure or security should be promptly directed to the Privacy Officer.

REFERENCES/CITATIONS
See 45 CFR §§160.103, 164.502(e), 164.504(e)

PLAN SPONSOR/ADEQUATE SEPARATION

POLICY

Health Plan shall amend its Plan Documents to restrict Uses and Disclosures of PHI by the Plan Sponsor, consistent with the requirements of the Privacy Rules. Health Plan shall require the Plan Sponsor to certify that it agrees to all requirements in 45 CFR §164.504(f)(2)(ii).

PROCEDURE

Health Plan may disclose Summary Health Information to the Plan Sponsor at any time for the purpose of: (1) obtaining premium bids from Insurers for providing health insurance coverage, or (2) modifying, amending, or terminating Health Plan.

Health Plan may also Disclose to the Plan Sponsor or a Member at any time information on whether an Individual is participating in Health Plan, or is enrolled in or has dis-enrolled from a health insurance issuer or HMO offered by Health Plan.

Health Plan may Disclose PHI to the Plan Sponsor or a Member to carry out Plan Administration Functions, provided Health Plan has received certification by Plan Sponsor as required by HIPAA.

Health Plan shall not Disclose PHI to the Plan Sponsor or a Member for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor or a Member.

REFERENCES/CITATIONS
See 45 CFR §§164.502(a)(5), 164.504(a), 164.504(f)

NOTICE OF PRIVACY PRACTICES

POLICY

Health Plan shall maintain a Notice of Privacy Practices, written in plain language, which contains all HIPAA required elements. Health Plan shall provide the Notice of Privacy Practices to any person on request, to Individuals covered by Health Plan, and to new enrollees in accordance with HIPAA timelines. Health Plan shall retain copies of all notices issued.

PROCEDURE

Any party requesting Health Plan's Notice of Privacy Practices shall be promptly provided a copy. Dates and times of requests and provisions shall be documented.

A paper copy of the Notice of Privacy Practices shall be provided to new enrollees at the time of enrollment.

At least once every three (3) years, a notice that Health Plan's Notice of Privacy Practices is available and how it may be obtained shall be provided to Individuals covered by Health Plan.

REFERENCES/CITATIONS
45 CFR § 164.520

RESTRICTION REQUESTS

POLICY

Individuals shall be allowed to request that Health Plan restrict Uses or Disclosures of their PHI for Treatment, Payment or Health Care Operations, or Disclosures to family, friends or others for involvement in care and notification purposes.

PROCEDURE

Individuals are notified of their right to request restrictions on how their PHI is Used and/or Disclosed for Payment and Health Care Operations in the Notice of Privacy Practices.

Requests for restriction must be made in writing. A Request to Restrict Use or Disclosure of PHI form shall be provided to any Individual upon request.

Health Plan may agree to an Individual's request for restrictions on the Use and Disclosure of his or her PHI if the request is determined to be reasonable. However, Health Plan does not have to agree to any restriction requests.

If a request for restriction is accepted, Privacy Officer shall notify appropriate Workforce members and Business Associates.

An agreed upon restriction may be terminated if the Individual agrees in writing, or if orally that fact is documented, or if Health Plan informs the Individual, and then only with respect to PHI created or received by Health Plan after the termination.

Privacy Officer shall notify Individuals of Health Plan's determination with respect to each such request.

REFERENCES/CITATIONS
45 CFR §§164.502(c), 164.522(a)

CONFIDENTIAL COMMUNICATION REQUESTS

POLICY

Individuals shall be allowed to request that Health Plan communicate PHI to the Individual by alternative means or at alternative locations. Health Plan shall accommodate reasonable requests if the Individual clearly states that other Disclosure could endanger them.

PROCEDURE

Individuals are notified of their right to request communication by alternative means or at alternative locations in the Notice of Privacy Practices and may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home.

A confidential communication request form shall be provided to any Individual upon request.

Such requests must be made in writing, specify an alternative address or other method of contact, and contain a statement that Disclosure could endanger the Individual.

If Health Plan grants an Individual's request, appropriate Workforce members and Business Associates shall be provided with the alternate communication requirements, promptly and in-writing.

REFERENCES/CITATIONS
45 CFR §§164.502(h), 164.522(b)

ACCESS TO INSPECT AND COPY PHI

POLICY

Individuals shall be permitted to request access to inspect and/or obtain a copy of PHI about them maintained in a Designated Record Set. Health Plan shall timely act to provide or deny the access in the manner required by HIPAA. Appropriate notice(s) shall be given of actions taken by Health Plan with respect to access requests. Documentation of all such access shall be retained.

PROCEDURE

Individuals are notified of their right to access to inspect and/or obtain a copy of PHI about them maintained in a Designated Record Set in the Notice of Privacy Practices.

Any Individual requesting access must do so in writing.

If the information requested is not the Individual's PHI or part of a Designated Record Set, the Individual has no right of access to it.

If Health Plan does not maintain the PHI that is the subject of a request, and Health Plan knows where the requested information is maintained, Health Plan shall inform the Individual where to direct the access request. Business Associates are required to Disclose PHI to Individuals, or their personal representatives, as necessary to satisfy Health Plan's access obligations.

Health Plan shall promptly notify Individuals of Health Plan's determination with respect to each such access request. Health Plan must act no later than thirty (30) days after receipt of the request. Health Plan may have a one-time extension of thirty (30) days if the Individual is given a written statement of the reason for the delay and the date by which Health Plan will complete its action on the request.

Denials

A request for access to any of the following may be denied without providing the Individual an opportunity for review:

i. Psychotherapy Notes;

ii. information compiled in reasonable anticipation of, or for use in civil, criminal, or administrative action or proceeding;

iii. PHI subject to the Privacy Act (5 U.S.C. §552a) if such denial is permitted thereunder; or

iv. PHI obtained from someone other than a health care provider under a promise of confidentiality, and providing access would reveal the source of the information.

A request for access may also be denied, but only if the Individual is provided an opportunity for review, when the access requested is reasonably likely to cause harm or endanger life or physical safety. Such review should be conducted by a licensed, independent (not otherwise involved) health care professional. Health Plan must allow/disallow access in accordance with this reviewing official's determination.

Health Plan shall, to the extent possible, give the Individual access to any other PHI requested, after excluding the PHI to which access is denied. Redacted information must be made completely unintelligible.

For requests denied, Health Plan must provide the Individual with a timely, written denial in plain language that contains:

a) The basis for the denial;

b) A statement of the Individual's right of review, if any, and how he or she may exercise that right;

c) a description of how the Individual may complain with Health Plan or the Secretary of HHS; and

d) the name or title, and telephone number of the Privacy Officer.

Acceptances

Before PHI is released, the identity of the person or entity requesting the information shall be verified.

If an Individual makes a valid, written request for access to PHI:

Health Plan shall provide the Individual with access to the information in the form or format requested, if it is readily producible. If it is not readily producible, the information may be produced in a readable hard copy format or as otherwise agreed between Health Plan and the Individual.

If an Individual requests personal access to inspect or copy, arrangements shall be made for a convenient time for inspection and copying of the records.

If an Individual requests that PHI be mailed, Health Plan shall honor that request if fees for copying and mailing are paid in advance. If the requested PHI may be provided more quickly/inexpensively in an electronic format, the Individual must be notified of this option.

Health Plan may discuss the scope, format and all other aspects of the access request with the Individual as necessary to facilitate its timely provision.

If the same PHI that is subject of the access request is maintained in more than one Designated Record Set or at more than one location, Health Plan need only produce the PHI once.

Health Plan may provide the Individual with a summary of the requested PHI, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided if the Individual agrees in advance to such summary or explanation and any fees.

If an Individual's access request directs Health Plan to transmit the copy of PHI directly to another entity or person, Health Plan shall do so, provided that request is in writing, signed by the Individual, and clearly identifies the designated person and where to send the copy.

Health Plan may charge the requestor a reasonable, cost-based fee for Disclosures of PHI, whether the information is provided in paper or electronically.

The Designated Record Sets that are subject to access by Individuals shall be documented.

REFERENCES/CITATIONS
45 CFR §§164.501, 164.502(a)(4)(ii), 164.514(h), 164.524

REQUESTS FOR AMENDMENT

POLICY

Individuals shall be permitted to request, in writing, that their PHI maintained in a Designated Record Set be amended. Health Plan shall timely act to grant or deny requests in accordance with HIPAA's requirements. Appropriate notice(s) shall be given of actions taken by Health Plan with respect to such requests. Individuals shall be permitted to submit written statements of disagreement to denials. Amendment requests, including on notice from another Covered Entity, and related documents shall be appended or linked to the PHI that is the subject of the request.

PROCEDURE

Individual requests for amendment of PHI must be made, in writing, and clearly identify the information to be amended, as well as the reasons for the amendment. These requirements are detailed in Health Plan's Notice of Privacy Practices.

Requests for amendment shall be acted upon promptly. Health Plan must act no later than sixty (60) days after receipt of the amendment. Health Plan may have a one-time extension of thirty (30) days for processing the amendment if the Individual is given a written statement of the reason for the delay and the date by which the amendment request will be processed.

Denials

A request for amendment may be denied if the material requested to be amended:

a) was not created by Health Plan, unless there is reasonable basis to believe the originator is no longer available to act on the request;
b) is not part of the Designated Record Set;
c) is not accessible to the Individual because federal and state law does not permit it; or
d) is accurate and complete.

If the request is denied, Health Plan must provide the Individual with a timely, written denial in plain language that contains:

a) the basis for the denial;
b) the Individual's right to submit a written statement disagreeing with the denial and how he or she may file such a statement;
c) a statement that if the Individual does not submit a statement of disagreement, he or she may request that Health Plan provide his or her request and the denial with any future Disclosures of the PHI that was the subject of the amendment;
d) a description of how the Individual may file a complaint with Health Plan or the Secretary of HHS; and
e) the name or title, and the telephone number of the Privacy Officer.

Health Plan must permit the Individual to submit a written statement disagreeing with the denial and the basis of such disagreement. Health Plan may reasonably limit the length of a statement of disagreement. Health Plan may prepare a written rebuttal to the Individual's statement of disagreement. If a rebuttal is prepared, Health Plan must provide a copy to the Individual.

Health Plan must, as appropriate, identify the record or PHI that is the subject of the disputed amendment and append or otherwise link in the Designated Record Set the Individual's request for amendment, Health Plan's denial of the request, the Individual's statement of disagreement, if any, and Health Plan's rebuttal, if any.

If an Individual submits a statement of disagreement, Health Plan must include the material appended or an accurate summary of such information with any subsequent Disclosure of PHI to which the disagreement relates. If an Individual does not submit a written statement of disagreement, Health Plan must include the request for amendment and its denial, or an accurate summary of such information, with any subsequent Disclosure of PHI only if the Individual has requested such action. When a subsequent Disclosure is made using a standard transaction that does not permit the additional material to be included, Health Plan may separately transmit the material required.

Acceptances

If the request to amend is granted, in whole or in part, Health Plan must:

a) insert the amendment or provide a link within the Designated Record Set to the amendment at the site of the information that is the subject of the request;
b) timely inform the Individual that the amendment is accepted;
c) obtain the Individual's identification of and agreement to have Health Plan notify the relevant persons with whom the amendment needs to be shared; and
d) within a reasonable time frame, make reasonable efforts to provide the amendment to persons identified by the Individual, and persons, including Business Associates, that Health Plan knows have the PHI that is the subject of the amendment and that may have relied on or could foreseeably rely on the information to the detriment of the Individual.

REFERENCES/CITATIONS
45 CFR §§160.306, 164.520, 164.524, 164.526, 164.530(d)

ACCOUNTINGS

POLICY

Individuals shall be permitted to request, in writing, an accounting of Disclosures of their PHI made by Health Plan in the past six (6) years. Health Plan shall timely act to provide the Individual with a written accounting containing only the appropriate HIPAA required content. Documentation of the accounting shall be retained.

PROCEDURE

Individuals who request an accounting shall complete and submit a written request. An Individual may request an accounting for any period of less than six years from the date of the request.

Health Plan must provide the accounting no later than sixty (60) days after receipt. Health Plan may extend the time once, by no more than thirty (30) days, as long as the Individual is provided with a written statement of the reasons for delay and the date by which Health Plan will provide the accounting.

Accountings are not required to include any of the following Disclosures:

- to carry out Treatment, Payment and Health Care Operations
- to Individuals regarding their own PHI
- pursuant to a signed authorization by the Individual or Individual's personal representative
- for national security or intelligence purposes
- to correctional institutions, law enforcement officials, or health oversight agencies
- incidental to a permitted Use or Disclosure
- that occurred as part of a limited data set

For each Disclosure, the accounting shall include:

- the date of the Disclosure;
- name of entity or person who received the PHI and, if known, their address
- a brief description of the PHI Disclosed; and
- a brief statement of the purpose of the Disclosure that reasonably informs the Individual of the basis for the Disclosure, or a copy of the written request for Disclosure, if any.

If there are multiple Disclosures of PHI to the same person or entity for a single purpose, the accounting may provide:

- the date, name, address, brief description and statement of purpose of the first Disclosure during the accounting period;
- the frequency, or number of Disclosures made during the accounting period; and
- the date of the last such Disclosure during the accounting period.

Once a year, Individual's may receive an accounting without cost. A reasonable cost-based fee may be imposed for each subsequent request within a 12-month period. Individuals shall be notified at the time of their first accounting request that such a fee will be imposed. Individuals shall be provided opportunity to withdraw or modify their request for subsequent accountings in order to avoid or reduce the fee.

Health Plan may temporarily suspend an Individual's right to receive an accounting if a health oversight agency or law enforcement requests it to do so.

The accounting request and a copy of the accounting provided should be retained.

REFERENCES/CITATIONS
45 CFR § 164.528

COMPLIANCE

POLICY

Health Plan shall cooperate with HHS in its conduct of compliance reviews.

PROCEDURE

Health Plan shall keep such records and submit such compliance reports as the Secretary of HHS may determine to be necessary to ascertain compliance.

Health Plan must permit access by the Secretary of HHS to its facilities, books, records, accounts and other sources of information (including PHI) that are pertinent to ascertaining compliance. If any information required is in the exclusive possession of another party that has failed or refused to furnish it, Health Plan shall so certify and set forth what efforts it has made to obtain the information.

REFERENCES/CITATIONS
45 CFR §§160.308, 160.310, 164.502(a)

MITIGATION

POLICY

Health Plan shall mitigate, to the extent practicable, any harmful effect that is known to it due to a Use or Disclosure of PHI by Workforce members or Business Associates in violation of these Policies and Procedures or the Privacy Rules.

PROCEDURE

Workforce members who become aware of a Use or Disclosure of PHI not in compliance with HIPAA or these Policies and Procedures, whether by their own action, by another Workforce member or by an outside consultant/contractor, shall immediately contact the Privacy Officer.

Privacy Officer shall promptly document any such report, look into relevant facts surrounding the Use or Disclosure in question, and, if possible, collect/limit any Unsecured PHI. Privacy Officer may consult with legal counsel for Health Plan.

If the suspected non-compliant Use or Disclosure relates to an outside consultant/contractor, Privacy Officer shall consult any applicable Business Associate Agreement to determine whether it contains more specific requirements regarding cooperation and efforts to mitigate.

Reasonable mitigating steps shall be quickly implemented based on prudent judgment, and considering Health Plan's knowledge of: (a) to whom PHI has been Disclosed, (b) how the information might be used for harm, and (c) what steps can actually have a mitigating effect with respect to the particular situation.

REFERENCES/CITATIONS
45 CFR §§164.504(e), 164.530(f)

BREACH NOTIFICATION

POLICY

Health Plan shall, following the discovery of a Breach of Unsecured PHI, promptly notify each Individual whose Unsecured PHI has been (or is reasonably believed by Health Plan to have been) accessed, acquired, Used, or Disclosed as a result of such Breach. A log of any such Breaches shall be maintained and notifications made to the Secretary of HHS and media as required.

PROCEDURE

Workforce members are encouraged to quickly report any suspected Breach of PHI.

Privacy Officer, on report of any Breach, should do all the following:

- Make inquiries to understand the nature of the Breach, including:

    1) Has there been an impermissible Use or Disclosure?
    2) Is the information at issue Unsecured PHI?
    3) What is the nature and extent of Unsecured PHI involved?
    4) What are the types of identifiers and the likelihood of re-identification?
    5) Was the PHI actually acquired or viewed?
    6) Who are the unauthorized person(s) who Used the PHI or to whom the Disclosure was made?
    7) Is the unauthorized recipient(s) obligated to protect the PHI?
    8) To what extent has the risk to the PHI been mitigated?

- Consult any applicable Business Associate Agreement to determine whether it contains more specific requirements regarding Breach (for example, short notification timeframes or requirements that Business Associate notify affected Individuals on Health Plan's behalf);

- Consult with legal counsel for Health Plan to determine whether a Breach has occurred;

- Request improper recipient's satisfactory assurances that the information will not be further Used or Disclosed (through a confidentiality agreement or similar means) or will be destroyed; and

- Document the investigation in writing.

Privacy Officer shall maintain a log of all discovered Breaches and provide a notice to the Secretary of HHS of the same, if any, by March 1 of each calendar year.

Breach notifications to affected Individuals, if any, shall be written in plain language, shall not contain PHI, and be completed by first-class mail (or e-mail if appropriate) to last known

addresses, without unreasonable delay and in no case later than sixty (60) calendar days after Breach Discovery.

Individual notices shall contain:

- A brief description of what happened, including dates;
- A description of the types of Unsecured PHI involved in the Breach;
- Steps Individuals should take to protect themselves from potential Breach harm;
- A brief description of what Health Plan is doing to investigate the Breach, mitigate harm, and to protect against further Breach; and
- Contact procedures for questions/further information.

Breach notifications involving five hundred (500) or more Individuals have additional notice requirements (to the media and the Secretary of HHS) which should be made after careful deliberation, but with the same content and timelines as those applicable to Individual Breach notifications (see above).

REFERENCES/CITATIONS
45 CFR §§164.400–414, 164.530(i)