HIPAA PRIVACY USE AND DISCLOSURE PROCEDURES

Introduction

Illinois Educators Risk Management Program Association (the "Association") sponsors the Illinois Educators Risk Management Program Group Health Plan (the "Plan")

Members of the Association or its participating Employers workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the Association or Employer, for administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Association's and Employer's ability to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

It is the Association's and Employers' policy to comply fully with HIPAA's requirements. To that end, all representatives and members of the workforce of these entities who have access to PHI must comply with these Use and Disclosure Procedures. For purposes of these Use and Disclosure Procedures and the Association's separate privacy policy, the workforce of these entities includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Association or an Employer, whether or not they are paid by the Association or Employer. The term "employee" includes all of these types of workers. Additionally, any subcontractors that provide services to the Business Associate which involve the creation, receipt, maintenance, or transmission of private health information on behalf of the Business Associate to fulfill its contractual duties, must comply fully with HIPAA's requirements.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by these Use and Disclosure Procedures. The Association reserves the right to amend or change these Use and Disclosure Procedures at any time (and even retroactively) without notice. To the extent these Use and Disclosure Procedures establish requirements and obligations above and beyond those required by HIPAA, these Use and Disclosure Procedures shall be aspirational and shall not be binding upon the Plan, the

Association, or an Employer. These Use and Disclosure Procedures do not address requirements under other federal laws or under state laws.

These procedures shall apply to all business associates of the Plan, including Health Alliance. However, Health Alliance may use its own forms and security policies and procedures, provided such forms, policies, and procedures comply with the HIPAA privacy and security requirements.

Procedures for Use and Disclosure of PHI

I. Use and Disclosure Defined

The Association, Employers, and the Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- Use. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any Plan representative, or person working for or within the human resources department of the Employer, or by a Business Associate (defined below) of the Plan.

- Disclosure. For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to Plan representative or persons not employed by or working within the human resources department of the location(s) of the Employer.

II. Workforce Must Comply With Employer's Policy and Procedures

All Plan representatives and members of the Employers' workforce (described at the beginning of these Use and Disclosure Procedures and referred to herein as "employees") must comply with these Use and Disclosure Procedures and the Employer's separate privacy policy.

III. Access to PHI Is Limited to Certain Employees

The following employees ("employees with access") have access to PHI:

- Those employees who perform functions directly on behalf of the Plan, and

- Any other employee who has access to PHI on behalf of the Employer for its use in “plan administrative functions”.

These employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum

amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) except in accordance with these Use and Disclosure Procedures.

IV. Permitted Uses and Disclosures of PHI: Payment and Health Care Operations

Definitions

Payment. Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- 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.

Health Care Operations. 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 plan performance;
- underwriting and premium rating;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development;
- business management and general administrative activities;
- to de-identify the information in accordance with HIPAA Rules as necessary to perform required services.

Procedure

- Uses and Disclosures for Plan's Own Payment Activities or Health Care Operations. An employee may use and disclose a Plan participant's PHI to perform the Plan’s own payment activities or health care operations.

- Disclosures must comply with the "Minimum-Necessary" Standard. (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Officer.)

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

- Disclosures for Another Entity's Payment Activities. An employee may disclose a Plan participant's PHI to another covered entity or health care provider to perform the other entity's payment activities. These disclosures will be made according to procedures developed by the Privacy Officer.

- Disclosures for Certain Health Care Operations of the Receiving Entity. An employee may disclose PHI for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the individual and the PHI requested pertains to that relationship. Such disclosures are made according to procedures developed by the Privacy Officer.

- The disclosure must be approved by the Privacy Officer.

- Disclosures must comply with the "minimum-Necessary Standard."

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

- Use or Disclosure for Purposes of Non-Health Benefits. Unless an authorization from the individual (as discussed in "Disclosures Pursuant to an Authorization") has been received, an employee may not use a participant's PHI for the payment or operations of the Employer's "non-health" benefits (e.g., disability, worker's compensation, and life insurance). If an employee requires a participant's PHI for the payment or health care operations of non-Plan benefits, follow the steps provided by the Privacy Officer.

- Obtain an Authorization. First, contact the Privacy Officer to determine whether an authorization for this type of use or disclosure is on file. If no form is on file, request an appropriate form from the Privacy Officer. **Employees shall not attempt to draft authorization forms.** All authorizations for use or disclosure for non-Plan purposes must be on a form provided by (or approved by) the Privacy Officer.

- Questions? Any employee who is unsure as to whether a task he or she is asked to perform qualifies as a payment activity or a health care operation of the Plan should contact the Privacy Officer or his or her designated representative.

V. Mandatory Disclosures of PHI: to Individuals and HHS

Procedure

- Request From Individual. Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own PHI, the employee must follow the procedure for "Disclosures to Individuals Under Right to Access Own PHI."

- Request From HHS. Upon receiving a request from a HHS official for disclosure of PHI, the employee must take the steps established by the Privacy Officer.

- Follow the procedures for verifying the identity of a public official set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

VI. Permissive Disclosures of PHI: for Legal and Public Policy Purpose

Procedure

- Disclosures for Legal or Public Policy Purposes. An employee who receives a request for disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Disclosures Covered" must contact the Privacy Officer. Disclosures may be made according to procedures established by the Privacy Officer.

- The disclosure must be approved by the Privacy Officer.

- Disclosures must comply with the "Minimum-Necessary Standard."

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Legal and Public Policy Disclosures Covered

- Disclosures about victims of abuse, neglect or domestic violence, if the following conditions are met:

    - The individual agrees with the disclosure; or

    - The disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual

is incapacitated and unable to agree and information will not be used against the individual and is necessary for an imminent enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

- For Judicial and Administrative Proceedings, in response to:

  - An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); and

  - A subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, upon receipt of assurances that the individual has been given notice of the request, or that the party seeking the information has made reasonable efforts to receive a qualified protective order.

- To a Law Enforcement Official for Law Enforcement Purposes, under the following conditions:

  - Pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.

  - Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.

  - Information about a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in the best interest of the individual.

  - Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.

  - Information that constitutes evidence of criminal conduct that occurred on the Association's or Employer's premises.

- To Appropriate Public Health Authorities for Public Health Activities.

- To a Health Oversight Agency for Health Oversight Activities, as authorized by law.

- To a Coroner or Medical Examiner About Decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law.

- For Cadaveric Organ, Eye or Tissue Donation Purposes, to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation.

- For Certain Limited Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.

- To Avert a Serious Threat to Health or Safety, upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.

- For Specialized Government Functions, including disclosures of an inmate's PHI to correctional institutions and disclosures of an individual's PHI to an authorized federal Official for the conduct of national security activities.

- For Workers' Compensation Programs, to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

VII. Disclosures of PHI Pursuant to an Authorization

Procedure

Disclosure Pursuant to Individual Authorization. Any requested disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required under these Use and Disclosure Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

- Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Verify that the authorization form is valid. Valid authorization forms are those that:

    - Are properly signed and dated by the individual or the individual's representative;

- Are not expired or revoked [the expiration date of the authorization form must be a specific date (such as July 1, 2016) or a specific time period (e.g., one year from the date of signature), or an event directly relevant to the individual or the purpose of the use or disclosure (e.g., for the duration of the individual's coverage)];

- Contain a description of the information to be used or disclosed;

- Contain the name of the entity or person authorized to use or disclose the PHI;

- Contain the name of the recipient of the use or disclosure;

- Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and

- Contain a statement regarding the possibility for a subsequent re-disclosure of the information.

- All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

VIII. Disclosure of PHI to Business Associates

Definition of Business Associate

Business Associate is an entity or person who:

- performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration; data analysis, underwriting, etc.); or

- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI;

Such Business Associates include:

- a health information organization;

- an e-prescribing gateway;

- another entity that provides data transmission services with respect to PHI to a covered entity and that requires routine access to PHI;

- is an entity that maintains PHI for a covered entity, whether or not the entity actually reviews the PHI.

Procedure

Use and Disclosure of PHI by Business Associate. All uses and disclosures by a "business associate" must be made in accordance with a valid business associate agreement. Before providing PHI to a business associate, employees must contact the Privacy Officer and verify that a business associate contract is in place.

The following additional procedures must be satisfied:

- Disclosures must be consistent with the terms of the business associate contract.

- Disclosures must comply with the "Minimum-Necessary Standard." (Under that procedure, each recurring disclosure will be subject to a separate policy to address the minimum-necessary requirement, and each non-recurring disclosure must be approved by the Privacy Officer.)

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

IX. Requests for Disclosure of PHI From Spouses, Family Members, and Friends

The Plan, Association, and Employer will not disclose PHI to family or friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member or friend, will be able to access PHI.

- If an employee receives a request for disclosure of an individual's PHI from a spouse, family member or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information."

- Once the identity of a parent or personal representative is verified, then follow the procedure for "Request for Individual Access."

- All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for "Disclosures Pursuant to Individual Authorization."

X. Disclosures of De-Identified Information

Definition of De-Identified Information

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. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

Procedure

- Obtain approval from the Privacy Officer for the disclosure. The Privacy Officer will verify that the information is de-identified.

- The Plan may freely use and disclose de-identified information. De-identified information is not PHI.

XI. Verification of Identity of Those Requesting Protected Health Information

Verifying Identity and Authority of Requesting Party. Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PHI of his or her minor child, a personal representative, or a public official seeking access.

- Request Made by Individual. When an individual requests access to his or her own PHI, the following steps should be followed:

    - Request a form of identification from the individual. Employees may rely on a valid driver's license, passport or other photo identification issued by a government agency.

    - Verify that the identification matches the identity of the individual requesting access to the PHI. If you have any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Officer.

    - Make a copy of the identification provided by the individual and file it with the individual's designated record set.

    - If the individual requests PHI over the telephone, ask for his or her social Security number.

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

- Request Made by Parent Seeking PHI of Minor Child. When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:

  - Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.

  - Disclosures must be documented in accordance with the procedure "Documentation Requirements."

- Request Made by Personal Representative. When a personal representative requests access to an individual's PHI, the following steps should be followed:

  - Require a copy of a valid power of attorney or other documentation—requirements may vary state-by-state. If there are any questions about the validity of this document, seek review by the Privacy Officer.

  - Make a copy of the documentation provided and file it with the individual's designated record set.

  - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

- Request Made by Public Official. If a public official requests access to PHI, and if the request is for one of the purposes set forth above in "Mandatory Disclosures of PHI" or "Permissive Disclosures of PHI," the following steps should be followed to verify the official's identity and authority:

  - If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set.

  - If the request is in writing, verify that the request is on the appropriate government letterhead.

  - If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for

services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

- Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Legal Department.

- Obtain approval for the disclosure from the Privacy Officer.

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

XII. Complying With the "Minimum-Necessary" Standard

Procedures for Disclosures

- Identify recurring disclosures. For each recurring disclosure, identify the types of PHI to be disclosed, the types of person who may receive the PHI, the conditions that would apply to such access, and the standards for disclosures to routinely-hired types of business associates. Create a policy for each specific recurring disclosure that limits the amount disclosed to the minimum amount necessary to accomplish the purpose of the disclosure.

- For all other requests for disclosures of PHI, contact the Privacy Officer, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Procedures for Requests

- Identify recurring requests. For each recurring request, identify the information that is necessary for the purpose of the requested disclosure and create a policy that limits each request to the minimum amount necessary to accomplish the purpose of the disclosure.

- For all other requests for PHI, contact the Privacy Officer, who will ensure the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Exceptions

- The "minimum-necessary" standard does not apply to any of the following:

    - Uses or disclosures made to the individual;

- Uses or disclosures made pursuant to an individual authorization;
- Disclosures made to HHS;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

XII. Documentation

Procedure

- Documentation. Employees shall maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:
  - “Notices of Privacy Practices" that are issued to participants;
  - Copies of policies and procedures;
  - Individual authorizations;
  - When disclosure of certain PHI is made:
    - the date of the disclosure;
    - the name of the entity or person who received the PHI and, if known, the address of such entity or person;
    - a brief description of the PHI disclosed;
    - a brief statement of the purpose of the disclosure; and
    - any other documentation required under these Use and Disclosure Procedures.

Note: The retention requirement only applies to documentation required by HIPAA. It does not apply to all medical records.

XIII. Mitigation of Inadvertent Disclosures of PHI

Mitigation: Reporting Required. HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to us of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this manual. As a result, if you become aware of a disclosure of PHI, either by an employee of Plan or an outside consultant/contractor, that is not in compliance with the policies and procedures set forth in this manual, immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the individual can be taken.

XIV. Breach Notification Requirements

Compliance: The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

Notification to Individuals

(a)(1) *General rule*. The Plan shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the Plan to have been, accessed, acquired, used, or disclosed as a result of such breach. (2) *Breaches treated as discovered.* For purposes of paragraph (a)(1), a breach shall be treated as discovered by the Plan as of the first day on which such breach is known to the Plan, or, by exercising reasonable diligence would have been known to the Plan. The Plan shall be deemed to have knowledge of a breach if such breach is known, or be exercising reasonable due diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the Plan or Association (determined in accordance with the federal common law of agency).

(b) *Timeliness of notification.* The Plan shall provide the notification required by paragraph (a) without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Content of notification*. The notification required by paragraph (a) shall include, to the extent possible: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (2) a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (3) any steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the Plan involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

(d) *Methods of Individual Notification*. The notification required by paragraph (a) shall be provided in the following form: (1) *Written notice.* (i) Written notification by first-class mail to the individual at the last known address of the individual, or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as

information is available. (ii) If the Plan knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available. (2) *Substitute notice*. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i), a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual. (i) in the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means. (ii) in the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the website of the Plan, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) Include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach. (3) *Additional notice in urgent situations.* In any case deemed by the Plan to require urgency because of possible imminent misuse of unsecured protected health information, the Plan may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under this section.

Notification to the Media

(a) *Notification*. For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, the Plan shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b) *Timeliness of notification.* Except as provided in the regulations, the Plan shall provide the notification required by paragraph (a) above without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

Notification to the Secretary

(a) *Notification.* The Plan shall, following the discovery of a breach of unsecured protected health information, notify the Secretary of Health and Human Services. (b) *Breaches involving 500 or more individuals.* For breaches of unsecured protected health information involving 500 or more individuals, the Plan shall, provide the notification required by paragraph (a) contemporaneously with the notice required by Section 7(a) and in the manner specified on the HHS Web site. (c) *Breaches involving less than 500 individuals.* For breaches of unsecured protected health information involving less than 500 individuals, the Plan shall

maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

Notification by a Business Associate

(a) *Standard*. (1) A business associate shall, following the discovery of a breach of unsecured protected health information, notify the Plan of such breach. (2) *Breaches treated as discovered.* For purposes of paragraph (1), a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if 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 an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency). (b) *Timeliness of notification.* A business associate shall provide the notification required by paragraph (a) without reasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) *Content of notification.* (1) The notification required by paragraph (a) shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. (2) A business associate shall provide the Plan with any other available information that the Plan is required to include in notification to the individual at the time of the notification required by paragraph (a) or promptly thereafter as information becomes available.

Law Enforcement Delay

If a law enforcement official states to the Plan or business associate that a notification, notice, or posting required under this policy would impede a criminal investigation or cause damage to national security, the Plan or business associate shall: (a) if the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) if the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) is submitted during that time.

Procedures for Complying With Individual Rights

Individual Rights: HIPAA gives individuals the right to access and obtain copies of their protected health information that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that individuals may request to have their

PHI amended, and that they are entitled to an accounting of certain types of disclosures.

I. Individual's Request for Access

"Designated Record Set" Defined

Designated Record Set is a group of records maintained by or for the Plan that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- other protected health information used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or from a minor's parent or an individual's personal representative) for disclosure of an individual's PHI, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Review the disclosure request to determine whether the PHI requested is held in the individual's designated record set. See the Privacy Officer if it appears that the requested information is not held in the individual's designated record set. No request for access may be denied without approval from the Privacy Officer.
- Review the disclosure request to determine whether an exception to the disclosure requirement might exist; for example, disclosure may be denied for requests to access psychotherapy notes, documents compiled for a legal proceeding, information compiled during research when the individual has agree to denial of access, information obtained under a promise of confidentiality, and other disclosures that are determined by a health care professional to be likely to cause harm. See the Privacy Officer if there is any question about whether one of these exceptions applies. No request for access may be denied without approval from the Privacy Officer.
- Respond to the request by providing the information or denying the request within 30 days. If the requested PHI cannot be accessed within the 30-day period, the deadline may be extended for 30 days by providing written notice

to the individual within the original 30 -day period of the reasons for the extension and the date by which the Plan will respond.

- A Denial Notice must contain (1) the basis for the denial; (2) a statement of the individual's right to request a review of the denial, if applicable; and (3) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Officer.

- Provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual.

- Individuals have the right to receive a copy by mail or by e-mail or can come in and pick up a copy. Individuals (including inmates) also have the right to come in and inspect the information.

- If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, prepare such summary and explanation of the information requested and make it available to the individual in the form or format requested by the individual.

- Charge a reasonable cost-based fee for copying, postage, and preparing a summary (but the fee for a summary must be agreed to in advance by the individual). This provision is not needed if the plan will not charge a fee.

- Disclosures must be documented in accordance with the procedure "Documentation Requirements."

II. Individual's Request for Amendment

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for amendment of an individual's PHI held in a designated record set, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Review the disclosure request to determine whether the PHI at issue is held in the individual's designated record set. See the Privacy Officer if it appears that the requested information is not held in the individual's designated record

set. No request for amendment may be denied without approval from the Privacy Officer.

- Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (see the access procedures above). See the Privacy Officer if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Officer**.**

- Review the request for amendment to determine whether the amendment is appropriate—that is, determine whether the information in the designated record set is accurate and complete without the amendment.

- Respond to the request within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Plan will respond.

- When an amendment is accepted, make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the unconnected information to the detriment of the individual.

- When an amendment request is denied, the following procedures apply:

    - All notices of denial must be prepared or approved by the Privacy Officer. A Denial Notice must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial.

    - If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement, if any; and the Employer's rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its

denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

III. Processing Requests for an Accounting of Disclosures of Protected Health Information

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosures, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- If the individual requesting the accounting has already received one accounting within the 12 month period immediately preceding the date of receipt of the current request, prepare a notice to the individual informing him or her that a fee for processing will be charged and providing the individual with a chance to withdraw the request.

- Respond to the request within 60 days by providing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below). If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Employer will respond.

- The accounting must include disclosures (but not uses) of the requesting individual's PHI made by Plan and any of its business associates during the period requested by the individual up to six years prior to the request. (Note, however, that the Plan is not required to account for any disclosures made prior to April 14, 2004.) The accounting does not have to include disclosures made:

    - to carry out treatment, payment and health care operations;

    - to the individual about his or her own PHI;

    - incident to an otherwise permitted use or disclosure;

    - pursuant to an individual authorization;

- for specific national security or intelligence purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without an authorization; and
- as part of a limited data set.

- If any business associate of the Plan has the authority to disclose the individual's PHI, then Privacy Officer shall contact business associate to obtain an accounting of the business associate's disclosures.
- The accounting must include the following information for each reportable disclosure of the individual's PHI:
  - the date of disclosure;
  - the name (and if known, the address) of the entity or person to whom the information was disclosed;
  - a brief description of the PHI disclosed; and
  - a brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)
- If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of disclosures of PHI would be reasonably likely to impede the agency's activities, disclosure may not be required. If an employee receives such a statement, either orally or in writing, the employee must contact the Privacy Officer for more guidance.
- Accountings must be documented in accordance with the procedure for "Documentation Requirements."

IV. Processing Requests for Confidential Communications

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

- The employee should take steps to honor requests.

- If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

- All confidential communication requests that are approved must be tracked.

- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

V. Processing Requests for Restrictions on Uses and Disclosures of Protected Health Information

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for access to an individual's PHI, the employee must take the following steps: Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- The employee should take steps to honor requests.

- If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

- All requests for limitations on use or disclosure of PHI that are approved must be tracked.

- All business associates that may have access to the individual's PHI must be notified of any agreed-to restrictions.

Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."