

**HIPAA Privacy Use and Disclosure Procedures  
Kentucky Retirement Systems**

**Effective: 01/01/2006**

**Revised as of: 09/23/2009, 02/17/2010, and 8/18/2011**

**Introduction**

Kentucky Retirement Systems (the Agency) sponsors and administers group health plans named the Kentucky Retirement Systems Health Plan – Medical Only, the Kentucky Retirement Systems Health Plan – Essential, and the Kentucky Retirement Systems Health Plan – Premium (the Plan). Members of the Agency’s 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 Agency, for administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Agency’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 includes information in any format (e.g., verbal, written or electronic).

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) was passed under the American Recovery and Reinvestment Act of 2009. The HITECH Act updates HIPAA privacy rules to include breach notification requirements, effective September 23, 2009, and to update other HIPAA privacy standards and to make such standards applicable to business associates of the Plan in the same way HIPAA applies to the Plan, generally effective August 18, 2011.

It is the Agency’s policy to comply fully with HIPAA’s requirements, as updated by the HITECH Act. To that end, all members of the Agency’s workforce who have access to PHI must comply with these Use and Disclosure Procedures. For purposes of these Use and Disclosure Procedures and the Agency’s HIPAA Privacy Policy, the Agency’s workforce 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 Agency, whether or not they are paid by the Agency. The term “employee” includes all of these types of workers.

The Agency will treat member account information, which may or may not be PHI, in a confidential manner pursuant to KRS 61.661 and, to the extent PHI is involved, the HIPAA Privacy Rule. Requests for member account information shall be subject to Agency policies developed pursuant to KRS 61.661 and as described herein.

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 Agency 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 Agency. These Use and Disclosure Procedures do not address requirements under other federal laws or under state laws.

**How These Use and Disclosure Procedures Are Organized:** These Use and Disclosure Procedures include two Parts.

“Procedures for Use and Disclosure of PHI” includes the use and disclosure procedures that must be followed when PHI will be used or disclosed for the Plan’s own payment and health care operations purposes and when PHI will be disclosed to third parties (but not the individual).

“Procedures for Complying With Individual Rights” includes procedures for complying with an individual’s right to access, amendment, and accounting of PHI held in a designated record set. This section also includes procedures for addressing individual requests for confidential communications and for limits on use and disclosure.

## Procedures for Use and Disclosure of PHI

### I. Use and Disclosure Defined

The Agency 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 person working within the Agency.
- **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 persons not employed by or working within the Agency.

### II. Workforce Must Comply With Agency’s Policy and Procedures

All members of the Agency’s 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 Agency’s HIPAA Privacy Policy.

### III. Access to PHI Is Limited

The following employees (“employees with access”) have access to significant amounts of PHI:

- *HIPAA Privacy Official* who has general oversight responsibility for the Agency’s HIPAA privacy practices and performs various other administrative functions directly on behalf of the Plan;
- *HIPAA Security Official* who performs data security functions and other administrative functions directly on behalf of the Plan;
- *Business Associates:* The Division of Retiree Healthcare (RHC) will provide enrollment and termination information (including name, social security number, address, date of birth, Medicare status, and effective date) to business associates as needed to enroll and dis-enroll members and dependents in a timely manner.
- *RHC Call Center and Division of Retiree Healthcare:* The RHC Call Center and Division of Retiree Healthcare Services will respond to inquiries from members and their personal representatives as to enrollment options, enrollment status, premiums due, and general plan design issues. Inquiries about the status of a particular claim, how to file a claim, availability of network providers, deductible and out-of-pocket status, covered and excluded procedures, formularies, and other specifics of the member’s plan coverage will be directed to the third party administrator or pharmacy benefits manager.

Inquiries that the third party administrator or pharmacy benefits manager is unable to respond to, or unable to respond to in a manner satisfactory to the member, will be directed to the manager for RHC

- *Senior Advisor Retiree Health Care*: The Senior Advisor, Retiree Health Care and his/her staff shall disclose only de-identified, summary information about use of plan resources to the Executive Staff, the Board, and other individuals responsible for managing the Plan.
- *Internal audit staff* when conducting HIPAA compliance audits; and
- *Members of Legal Services staff* who will have access to PHI on behalf of the Agency for the purpose of providing advice related to receipt, use, and disclosure of PHI and other legal issues involving health insurance.
- For all other requests for disclosures of PHI, contact the Privacy Official, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

□ 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.

Other employees have access to limited amounts of PHI (*i.e.*, no diagnosis or other medical information) as described below in these Use and Disclosure Procedures.

#### **IV. Permitted Uses and Disclosures of PHI: Payment, Treatment and Health Care Operations**

**OBJECTIVE:** Facilitate use or disclosure of PHI for payment purposes, treatment activities, and health care operations under circumstances permitted by HIPAA.

##### **Definitions**

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

- eligibility and coverage determinations including coordination of benefits or the determination of cost sharing amounts, and adjudication or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics;

- billing, claims management, collection activities, obtaining payment under any contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing;
- review of health care services with respect to medical necessity, coverage under a health plan, appropriateness or justification of charges;
- utilization review activities, including precertification and preauthorization of services and concurrent and retrospective review of services; and
- disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:
  - name and address;
  - date of birth;
  - Social Security number;
  - payment history;
  - account number; and
  - name and address of the health care provider and/or health plan.

***Treatment.*** Treatment means the provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

***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, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

- underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the health plan receiving individually identifiable health information does not disclose such information if the insurance or benefits are not placed with it;
- conducting or arranging for medical review, legal services, and auditing functions and compliance programs;
- business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
- business management and general administrative activities, including, but not limited to:
  - management activities relating to implementation of and compliance with the requirements of the HIPAA regulations;
  - customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer;
  - resolution of internal grievances;
  - the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that, following such activity, will become a covered entity and due diligence related to such activity; and
  - creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

### **Procedure**

- *Uses and Disclosures for Plan's Own Payment Activities or Health Care Operations, or the Health Care Operations of Any Other Covered Entity That Participates With the Plan in an Organized Health Care Arrangement.* An employee may use and disclose a Plan participant's PHI to perform the Plan's own payment activities or health care operations (or the health care operations of any other covered entity that participates with the Plan in an organized health care arrangement).
- Disclosures must comply with the "Minimum-Necessary Standard." (Under that procedure, if the disclosure is not routine, the disclosure must be approved by the Privacy Official.)

- Non-routine 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. Disclosures may be made under the following procedures:
  - Disclosures must comply with the “Minimum-Necessary Standard.” (Under that procedure, if the disclosure is not routine, the disclosure must be approved by the Privacy Official.)
  - Non-routine disclosures must be documented in accordance with the procedure for “Documentation Requirements.”
- *Disclosures for Treatment Activities.* An employee may disclose PHI for treatment activities of a health care provider. Disclosures may be made under the following procedures:
  - Disclosures must comply with the “Minimum-Necessary Standard.” (Under that procedure, if the disclosure is not routine, the disclosure must be approved by the Privacy Official.)
  - Non-routine disclosures must be documented in accordance with the procedure for “Documentation Requirements.”
- *Disclosures for Certain Health Care Operations of the Receiving Entity.* An employee may disclose PHI for the following purposes if the other covered entity has (or had) a relationship with the individual and the PHI requested pertains to that relationship:
  - Detection of fraud and abuse or health care compliance.
  - Conducting quality assessment and improvement activities (including outcomes evaluation and development of clinical guidelines), provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities.
  - Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, and related functions that do not involve treatment.
  - Reviewing the competence or qualifications of health care professionals.
  - Evaluating practitioner performance or health plan performance.

- Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers.
- Training of non-health care professionals.
- Accreditation, certification, licensing, or credentialing services.

Such disclosures are subject to the following:

- The disclosure must be approved by the Privacy Official.
- 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 Agency’s “nonhealth” benefits (e.g., disability, retirement benefits, and life insurance). If an employee requires a participant’s PHI for the payment or health care operations of non-Plan benefits, follow these steps:
  - Obtain an Authorization. First, contact the Privacy Official 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 Official. ***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 Official.
  - The disclosure must be approved by the Privacy Official.
  - Disclosures must comply with the authorization form.
- *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 their manager. Managers who need guidance to address the employee’s question should contact the Privacy Official.

**V. Mandatory Disclosures of PHI: to Individuals and U.S. Department of Health and Human Services**

OBJECTIVE: Facilitate disclosures when required by HIPAA to individuals upon request and to the U.S. Department of Health and Human Services (“DHHS”) for purposes of enforcing HIPAA.



## 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 DHHS.* Upon receiving a request from a DHHS official for disclosure of PHI, the employee must take the following steps:
  - 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 Purposes

OBJECTIVE: Facilitate disclosures for legal and public policy purposes under circumstances permitted by HIPAA.
--

### Definitions

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

A *public health authority* means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

### 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 Official. Disclosures may be made under the following procedures:

- The disclosure must be approved by the Privacy Official and must be consistent with 45 CFR § 164.512.
- 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* to a government authority (such as social services or protective services), if the following conditions are met:
  - The disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
  - The individual agrees with the disclosure; or
  - The disclosure is expressly authorized by statute or regulation and:
    - the Privacy Official, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual (or other victims); or
    - the individual is unable to agree because of incapacity and a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

If a disclosure is made without informing the individual, the individual must be promptly informed of the disclosure unless, in the professional judgment of the Privacy Official, this would place the individual at risk of serious harm, or involve a personal representative who is believed by the Privacy Official 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); or
  - A subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, upon receipt of assurances that one of the following sets of criteria has been satisfied:

- (i) The person seeking PHI has made reasonable efforts to ensure that the individual whose PHI is being sought has been given notice of the request. Such notice must be in writing and must also be provided to the Plan. It must contain sufficient information about the litigation or proceeding to which the PHI is sought to permit the individual to raise an objection to the court or administrative body. Before the disclosure is made, the party seeking the disclosure must also certify in writing to the Plan that the time for the individual to raise objections has expired and that no objections were filed or any objections were denied by the court or administrative body; or
  - (ii) The person seeking the PHI has made reasonable efforts to obtain a qualified protective order. It must be an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which it was requested and requires the return to the Plan or destruction of the PHI (including all copies made) at the end of the litigation or proceeding. The person seeking PHI must provide a written statement to the Plan that such an order has been secured (as well as a copy of the order) or that it has been requested.
- *To a Law Enforcement Official for Law Enforcement Purposes*, under the following conditions:
- Pursuant to a process and as otherwise required by law, the Plan may disclose PHI:
    - as required by law, including laws that require the reporting of certain types of wounds or other physical injuries; or
    - in compliance with and as limited by the relevant requirements of:
      - a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
      - a grand jury subpoena; or
      - an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
        - the information sought is relevant and material to a legitimate law enforcement inquiry;
        - the request is specific and limited to amounts reasonably practicable in light of the purpose for which the information is sought; and

- de-identified information could not reasonably be used.
- Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person. In such case, the Plan may disclose only the following information:
  - name and address;
  - date and place of birth;
  - Social Security number;
  - ABO blood type and rh factor;
  - type of injury;
  - date and time of treatment;
  - date and time of death, if applicable; and
  - a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
- Information about a suspected victim of a crime if:
  - the individual agrees to disclosure; or
  - the Plan is unable to obtain the individual's agreement because of Incapacity or other emergency circumstance, provided that:
    - the law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim, and
    - the disclosure is in the best interests of the individual, as determined by the Privacy Official, in the exercise of professional judgment.
- 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 Agency's premises.
- *To Appropriate Public Health Authorities for Public Health Activities* disclosures may be made for the following purposes:
  - To a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease,

injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

- To a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;
  - To a person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity; or
  - To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the Plan or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.
- *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 or an institutional review 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 inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials 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

OBJECTIVE: Facilitate disclosures of PHI as permitted by HIPAA when authorized by the individual whose PHI will be disclosed. PHI disclosed pursuant to an individual authorization may be disclosed for any purpose so long as the disclosure is consistent with the terms of the 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."
  - Submit the authorization to the Privacy Official, who will determine if the authorization 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, 2011] 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 description of each purpose of the requested use or disclosure; and
    - Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations.
  - In addition, the authorization must advise the individual of the following rights:

- The individual's right to revoke the authorization in writing, and any exceptions to the right to revoke (*i.e.*, as to disclosures that have already been made in reliance on the authorization or when the authorization was required as a condition for enrollment).
- The ability of the Plan to condition payment, enrollment, or eligibility for benefits on the authorization by stating either:
  - The Plan may not condition payment, enrollment, or eligibility for benefits on whether the individual signs the authorization; or
  - The consequences to the individual of a refusal to sign the authorization when the Plan can condition enrollment or eligibility for benefits on the individual's signing of the authorization;
- A statement that information disclosed pursuant to the authorization may potentially be subject to redisclosure by the party receiving the information and it may no longer be protected by state or federal privacy laws.
- The Plan and the third-party administrator will allow individuals to revoke an authorization at any time, in writing. If the Plan has already relied upon the authorization, or if the authorization was obtained as a condition for obtaining coverage, the authorization will not be revoked as to such matters.
- All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.

### **VIII. Disclosure of PHI to Business Associates**

OBJECTIVE: Verify that disclosure of PHI to business associates is consistent with a valid business associate contract.

#### **Definition of Business Associate**

A *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, administrative, accreditation, or financial services, where the performance of such services involves giving the service provider access to 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 Official 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 routine disclosures will be subject to analysis to address the minimum-necessary requirement, and each non-routine disclosure must be approved by the Privacy Official.)
  - Certain non-routine disclosures (*i.e.*, those made for a reason other than Payment, Treatment or Health Care Operations) must be documented in accordance with the procedure for “Documentation Requirements.”
- *Contents of business associate contracts.* The Plan's business associate contracts will, at a minimum:
  - establish the permitted and required uses and disclosures of PHI by the business associate;
  - permit the business associate to provide data aggregation services relating to the health care operations of the Plan; and
  - require the business associate to:
    - not use or further disclose the PHI except as allowed by the contract or as required by law and to limit any use or disclosure, or any request for PHI, to the minimum amount of PHI necessary to accomplish the purpose of the use, disclosure, or request;
    - use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by its contract;
    - comply with the security and privacy provisions made directly applicable to business associates under the HITECH Act;
    - report to the Plan any use or disclosure of the PHI not provided for under the contract;
    - provide such information as required within the timeline allowed by the contract in the case of a breach of unsecured PHI;



- censure that any agents or subcontractors to whom the business associate provides PHI received from, or created or received by the business associate on behalf of the Plan agree to the same restrictions and conditions that apply to the business associate with respect to such information;
  - make available PHI so that the Plan can satisfy its access, amendment, and accounting obligations to individuals;
  - make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of Health and Human Services for purposes of determining the Plan's compliance with HIPAA;
  - at termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the Plan that the business associate still maintains in any form and retain no copies of such information or, if not feasible, extend the protections of the contract to the information and limit further uses and disclosure to those purposes that make the return or destruction of the information infeasible; and
  - authorize termination of the contract and any other agreement with the business associate by the Plan, if either party determines that the other party has violated a material term of the contract.
- *Documentation.* The Privacy Official will maintain copies of each business associate contract for at least 6 years after the contract's final term ends.

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

OBJECTIVE: Protect privacy of individual's PHI by disclosing it only as authorized.

The Plan and Agency will not disclose PHI to family and friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including a spouse, family member or friend, will be able to access PHI. The Plan may disclose a limited amount of PHI (excluding diagnosis) in an explanation of benefits as part of the Plan's payment functions.

### **Procedure**

- 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."
- Except in emergency situations or under other circumstances approved by the Privacy Official, 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."
- In emergency situations or under other circumstances approved by the Privacy Official, the Plan may disclose PHI to people involved in an individual's care or payment for care if the Plan first: (1) informs the individual of the request and provides the individual with an opportunity to object to the disclosure; or (2) if the individual is not available, is incapacitated, or if an emergency exists, in the exercise of professional judgment, the Privacy Official determines that the disclosure is in the individual's best interest.

**X. Disclosures of De-Identified Information**

OBJECTIVE: Permit disclosure of de-identified information in accordance with HIPAA.

**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: (i) by professional statistical analysis; or (ii) by removing the following 18 specific identifiers:

- names;
- all geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
  - the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- telephone numbers;
- fax numbers;

- electronic mail addresses;
- Social Security numbers;
- medical record numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate/license numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- device identifiers and serial numbers;
- web Universal Resource Locators (URLs);
- internet Protocol (IP) address numbers;
- biometric identifiers, including finger and voice prints;
- full face photographic images and any comparable images; and
- any other unique identifying number, characteristic, or code, except as permitted for purposes of re-identification.

**Procedure**

- Obtain approval from Privacy Official prior to converting PHI into de-identified information and prior to making a disclosure of such information. The Privacy Official 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**

**OBJECTIVE:** Verify identity and authority of individual requesting access to PHI.

**Procedure**

- *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 drivers 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 Official.
- 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, the member's PIN must be provided before any PHI will be released.
- Non-routine 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. If the parent seeks information other than enrollment information from the Agency, the request must be reviewed by the Privacy Official and Legal Services. For requests for information related to information held by business associates, such as claims information or claims adjudication information, the requestor will be referred to the appropriate business associate.
  - 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, which addresses health care decisions.
  - 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 Official.
- Disclosures must be documented in accordance with the procedure for “Documentation Requirements.”

## **XII. Complying with the “Minimum-Necessary” Standard**

**OBJECTIVE:** Limit the PHI used, disclosed, or requested to the “minimum necessary” to accomplish the purpose of the use, disclosure, or request, unless an exception applies.

### **Definition of Minimum Necessary**

When using or disclosing PHI, or when requesting PHI from another covered entity (health care provider, health plan, or health care clearinghouse), employees must make reasonable efforts to limit PHI to the *minimum necessary* to accomplish the intended purpose of the use, disclosure, or request. Until such time as the Secretary of the Department of Health and Human Services issues guidance on what constitutes “minimum necessary,” employees will limit such PHI, to the extent practicable, to the limited data set in order to comply with the “minimum necessary” requirement, or, if needed by the Plan, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

## **Definition of Limited Data Set**

A *limited data set* is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- names;
- postal address information, other than town or city, State, and zip code;
- telephone numbers;
- fax numbers;
- electronic mail addresses;
- Social Security numbers;
- medical record numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate/license numbers;
- vehicle identifiers and serial numbers;
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers;
- biometric identifiers, including finger and voice prints; and
- full face photographic images and any comparable images.

## **Procedure**

The Plan has identified the following persons who need access to PHI to carry out their duties:

- Business Associates:* The Division of Retiree Healthcare (RHC) will provide enrollment and termination information (including name, social security number, address, date of birth, Medicare status, and effective date) to business associates as needed to enroll and dis-enroll members and dependents in a timely manner.
- RHC Call Center and Division of Retiree Healthcare:* The RHC Call Center and Division of Retiree Healthcare Services will respond to inquiries from members and their personal representatives as to enrollment options, enrollment status, premiums due, and general plan design issues. Inquiries about the status of a particular claim, how to file a claim, availability of network providers, deductible and out-of-pocket status, covered and excluded procedures, formularies, and other specifics of the member's plan coverage will be directed to the third party administrator or pharmacy benefits manager. Inquiries that the third party administrator or pharmacy benefits manager is

unable to respond to, or unable to respond to in a manner satisfactory to the member, will be directed to the manager for RHC

- *Senior Advisor Retiree Health Care*: The Senior Advisor, Retiree Health Care and his/her staff shall disclose only de-identified, summary information about use of plan resources to the Executive Staff, the Board, and other individuals responsible for managing the Plan.
- *HIPAA Privacy Official* who has general oversight responsibility for the Agency's HIPAA privacy practices and performs various other administrative functions directly on behalf of the Plan;
- *HIPAA Security Official* who performs data security functions and other administrative functions directly on behalf of the Plan;
- *Internal audit staff* when conducting HIPAA compliance audits; and
- *Members of Legal Services staff* who will have access to PHI on behalf of the Agency for the purpose of providing advice related to receipt, use, and disclosure of PHI and other legal issues involving health insurance.
- For all other requests for disclosures of PHI, contact the Privacy Official, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

#### **Procedures for Requests**

- RHC Call Center: If the member or personal representative knows the member's PIN, the RHC Call Center will release the member's effective date, plan coverage, and payment status to the inquiring party.
- Senior Advisor Retiree Health Care: The Senior Advisor Retiree Health Care and his/or her staff shall routinely report general plan usage information to the Board, but in no event may the staff disclose details of individual claims or claim usage. The Senior Advisor and staff shall assist business associates with requests for information that involve eligibility, enrollment and other coverage.
- For all other requests for PHI, contact the Privacy Official, who will ensure that 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:
  - Disclosures to or requests by a health care provider for treatment;
  - Uses or disclosures made to the individual;

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

### **XIII. Documentation Requirements**

**OBJECTIVE:** Comply with the HIPAA mandate to document uses and disclosures of PHI.

#### **Procedure**

- *Documentation.* The Privacy Official (or his/or her designated representative) shall maintain copies of all of the following items for a period of at least 7 years from the date created or 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 PHI is made under circumstances which, pursuant to these Use and Disclosure Procedures, require the disclosure to be documented in accordance with this "Documentation Requirements" procedure, maintain with respect to each such disclosure:
    - 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.

### **XIV. Mitigation of Inadvertent Disclosures of PHI**

**OBJECTIVE:** Comply with the HIPAA mandate to mitigate, to the extent possible, the harmful effects that result from an unlawful use or disclosure of an individual's PHI.



## **Procedure**

*Mitigation: Reporting Required.* HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to the Agency 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 an employee becomes aware of a disclosure of PHI, either by an employee of the 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 Official so that the appropriate steps to mitigate the harm to the individual can be taken.

## **XV. Delegation of Authority**

The Privacy Official shall obtain agreements to comply with the HIPAA Privacy, Transactions and Security Rules from all business associates prior to allowing the Plan to share PHI with the business associate. The Privacy Official shall maintain the business associate agreement for at least 7 years following termination of the business associate relationship.

As of January 1, 2010, UMR Inc. is the Plan's business associate for purposes of adjudicating claims, including handling appeals, coordinating benefits and pursuing third party liability, cutting benefits checks, and providing utilization management. Catalyst Rx, Inc. is the Plan's business associate for purposes of dispensing prescription drugs, including related utilization management and appeals. This Plan shall promptly refer all issues involving specific individuals to the appropriate business associate. The referral is made by explaining that a certain function or service is done by the business associate and helping the requestor understand how to contact the business associate.

## **XVI. Training**

**OBJECTIVE:** Comply with the HIPAA mandate to educate and train members of the Plan's workforce as to the appropriate manner of handling PHI in order to carry out their job functions and to appropriately sanction those members who fail to comply with the Plan's privacy policies and procedures.

## **Procedure**

- The Privacy Official (or his/her designated representative) will be responsible for identifying those individuals who perform a function for the Plan involving the use of PHI and are part of the Plan's workforce, as defined above. The Privacy Official will ensure that each member of the Plan's workforce receives training according to the following schedule:
  - (i) within a reasonable period of time after the person joins the Plan's workforce; and

- (ii) to each member of the Plan's workforce whose functions are affected by a material change in the policies or procedures, within a reasonable period of time after the material change becomes effective.
- The Plan will provide additional training as to the Plan's Policies and Procedures to any individual employee or business associate of the Plan, upon request.
- Training will involve an overview of the Plan's obligations under Privacy Regulations and the Plan's Policies and Procedures that are applicable to the members of the workforce being trained. The training may be presented in written and/or verbal form.
- The Privacy Official (or his/her designated representative) will document the content, date, and attendance at each of the training sessions as described above and will retain such documentation for at least 7 years from the date of creation, or the date it last was in effect, whichever is later.
- Members of the Plan's workforce who use or disclose an individual's PHI in violation of the training provided, the Privacy Regulations, or the Plan's Policies and Procedures will be subject to sanctions that will be consistent with the nature of the violation. Such sanctions may include, but are not be limited to, verbal and written warnings, suspensions, and termination. Sanctions will be imposed by the Agency in consultation with the Privacy Official who will document any sanctions that are imposed.

## **XVII. "Whistleblowing" and Workforce Member Crime Victims**

**OBJECTIVE:** To disclose PHI to appropriate individuals for purposes of reporting certain unlawful conduct or dangerous conditions in compliance with HIPAA.

### **Procedure**

- The Plan, a workforce member, or a business associate may disclose PHI without authorization from an individual to whom the information relates in the following circumstances:
  - if the workforce member or business associate believes in good faith that the Plan has engaged in conduct that is unlawful or otherwise violates professional standards, or that the services provided by the Plan potentially endanger one or more patients, workers, or the public; and
  - the disclosure is to:
    - a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Plan or to an appropriate health care accreditation organization

for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Plan; or

- an attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the relevant conduct.
- A workforce member who provides service to the Plan and who is the victim of a criminal act may disclose PHI to a law enforcement official if:
  - the information disclosed is about the suspected perpetrator of the criminal act; and
  - the information disclosed is limited to the following information:
    - name and address;
    - date and place of birth;
    - Social Security number
    - ABO blood type and rh factor;
    - type of injury;
    - date and time of treatment;
    - date and time of death, if applicable; and
    - a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

### **XVIII. Technical, Administrative and Physical Safeguards**

<b>OBJECTIVE:</b> Comply with the HIPAA's requirements to implement technical, administrative and physical safeguards with respect to PHI.
--

#### **Procedure**

The Plan shall use the following methods to protect PHI:

- (i) The Senior Advisor Retiree Healthcare shall maintain member enrollment information in a secure area. Employees will set computer screens to lock upon leaving their work stations.
- (ii) Counselors will close their doors when meeting with members. PHI shared by the member will not be recorded, unless needed to accomplish a legitimate Agency business function. Any recording of PHI will be performed subject to the "minimum necessary" standard described in these HIPAA Privacy Use and Disclosure

Procedures. His/her computer will be set to lock upon departure from the work station.

- (iii) The Senior Advisor Retiree Health Care and his/her staff will be seated in an isolated area. Personnel will close their doors when discussing PHI with members, business associates, or other members of the Agency in person or on the telephone. Member information will be maintained in locked drawers. His/her computer will be set to lock upon departure from the work station.
- (iv) The internal audit staff will maintain audit records containing PHI in a locked cabinet in a locked office. Audit records containing PHI will be retained for at least 7 years from the date created.
- (v) System security measures are addressed in the HIPAA Security Policy.
- (vi) The Agency is locked at all times, except during business hours at entrances designated for public access. At public access entrances, the receptionist will bar visitors from entering business areas unless the visitor is accompanied by an employee. Employees gain admittance with keys at locked doors at all entrances not designated for public access. Visitors are escorted at all times.

#### **XIX. Securing PHI and Notification in Case of Breach of Unsecured PHI**

OBJECTIVE: Comply with the HITECH Act's notification requirements in the event of a breach of unsecured PHI.
--

##### **Definitions**

*Breach* means the acquisition, access, use, or disclosure of PHI in a matter not permitted under the Privacy Regulations which compromises the security or privacy of the PHI. A breach excludes:

- Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the Plan or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Regulations.
- Any inadvertent disclosure by a person who is 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 the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Regulations.

- 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.

*Unsecured PHI* means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services in the guidance issued under the HITECH Act.

### **Procedure**

- To the extent practicable, the Plan will secure all PHI by rendering such PHI unusable, unreadable, or indecipherable to unauthorized individuals by either encryption or destruction, depending on what is appropriate for the circumstances. The notification requirements discussed in these Use and Disclosure Procedures will not apply to any PHI that is secured by one of the approved methods. In the event of a breach of PHI, the Privacy Official will determine if the breach relates to secured PHI, in which case the notification requirements will not apply, or if the breach relates to unsecured PHI, in which case the notification requirements will apply.
- The Privacy Official will be responsible for implementing reasonable systems for discovery of breaches of PHI, both internally and with the Plan's business associates, to ensure the timely compliance with all notice requirements in the event of a breach of unsecured PHI, including the following:
  - The Privacy Official will be responsible for ensuring that the Plan's workforce is trained to effectively identify and communicate any discovery of a breach of PHI (whether unsecured or secured). Workforce members who believe there may have been a breach of unsecured PHI shall notify the Privacy Official immediately.
  - Business associates are required by law to comply with the breach notification rules under the HITECH Act. The Plan will amend its contracts with business associates to appropriately define the role of the Plan and the business associate in the event of a breach of unsecured PHI.
  - The Privacy Official will be responsible for promptly investigating all reports of potential breaches of PHI and determining whether a breach has occurred, whether such breach involves unsecured PHI, and what additional information may be required to comply with all notice requirements in a timely manner.
- *Notification of individuals:*
  - Following the discovery of a breach of unsecured PHI, the Plan will notify each individual whose unsecured PHI has been, or is reasonably believed

by the Plan to have been, accessed, acquired, used, or disclosed as a result of such breach.

- The Plan will treat the date on which a breach of unsecured PHI is discovered as the first day that the breach is known to the Plan, or the first day on which the breach would have been known to the Plan had it been exercising reasonable diligence.
- Except in the case that law enforcement requests a delay, the Plan will send the required notification without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered by the Plan. In the case that the breach is first discovered by a business associate of the Plan, the Plan will send out the required notification no later than 60 calendar days after the business associate notifies the Plan of the breach.
- The notification provided to the individual will include the following information in plain language:
  - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
  - A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information);
  - Any steps individuals should take to protect themselves from potential harm resulting from the breach;
  - A brief description of what the Plan is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
  - 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.
- The Plan may provide the notification to each affected individual by electronic mail to such individuals who have agreed to receive notification by electronic mail, and for all others, the Plan will send the notification by first-class mail to each such individual's last known address. In the case that the Plan has insufficient or out-of-date contact information that precludes a written notification, the Plan may provide a substitute notice, which may be made by telephone if the Plan has insufficient contact information for fewer than 10 individuals. If the Plan has insufficient contact information for 10 or more individuals, it may provide notice through either a conspicuous posting on the Plan's website for 90 days that includes a toll-free number to call for further information, or a

conspicuous notice in major print or broadcast media in the geographic area where the individuals affected by the breach likely reside that includes a toll-free number that is active for at least 90 days. In any case deemed by the Privacy Official to require urgency, the Plan may, in addition to the above methods of notification, provide information to individuals by telephone or other appropriate means. The notification may be sent in more than one installment, as information regarding the breach becomes available.

- *Notification to the media:* The Plan will provide notice to prominent media outlets serving a state or jurisdiction in the event of a breach of unsecured PHI that affects or is reasonably believed to have affected more than 500 residents of such state or jurisdiction. The Plan will provide this notice in the form of a press release within the same timeframe that it provides individual notifications and containing the same information provided to affected individuals.
- *Notification to the Secretary of DHHS:* The Plan will notify the Secretary of DHHS of breaches of unsecured PHI. If the breach involves 500 or more individuals, the Plan will notify the Secretary within the same timeframe that it provides individual notifications. If the breach involves fewer than 500 individuals, the Privacy Official will maintain a log of such breaches and annually submit the log to the Secretary, within 60 days following the end of the calendar year in which the breaches occurred. The Plan will provide information about any breaches to the Secretary in the manner specified on the DHHS website.
- *Notification by a business associate:* The Plan will require, through appropriate amendment of its business associate contracts, that any business associate of the Plan that discovers a breach of unsecured PHI promptly notify the Plan of the breach so that the Plan can notify affected individuals. The Plan will further require the business associate to provide the Plan, to the extent possible, with the identification of each affected individual and any other available information that the Plan is required to include in notification to the individual. The business associate contracts will govern the timing and other details required of business associates in the event of a breach of unsecured PHI.
- *Law enforcement delay:* The Plan will delay the notification required under these Use and Disclosure Procedures if a law enforcement official states that notification will impede a criminal investigation or cause damage to national security. In the event such a delay is requested, the Privacy Official will document the request and the identity of the official making the statement.
- *Documentation of impermissible uses and disclosures:* In the case of any impermissible use or disclosure of PHI, the Privacy Official shall maintain documentation to demonstrate that all required notifications were made under

these Use and Disclosure Procedures, or, alternatively, that the impermissible use or disclosure did not constitute a breach of unsecured PHI, and, therefore, notifications were not required.

## **XX. Fundraising, Marketing, and Sale of PHI**

**OBJECTIVE:** Comply with HIPAA's (1) restrictions on fundraising and marketing with respect to an individual's PHI and (2) prohibition on the sale of PHI, as updated by the HITECH Act.

### **Definition of Marketing**

*Marketing* means either of the following:

- To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:
  - to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits;
  - for treatment of the individual; or
  - for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.
- An arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

### **Procedure**

- The Plan will not use or disclose PHI for the purpose of fundraising or marketing, nor will it receive any indirect or direct remuneration for any PHI.
- Marketing does not include communications made by the Plan to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Plan. Therefore, the Plan will continue to use and disclose PHI without the individual's authorization to communicate with individuals about entities participating in a



health care provider network or health plan network, about replacement of, or enhancements to the benefits offered by the Plan, and other health related products or services available only to Plan participants, and for case management or care coordination for the individual.

- Marketing further does not include any communications made by the Plan as described in the previous paragraph for which the Plan receives or has received direct or indirect payment in exchange for making such communications under the following circumstances:
  - Where such communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication, and any payment received by the Plan in exchange for making such communication is reasonable in amount; or
  - Where such communication is made by the Plan and the Plan obtains from the recipient of the communication a valid authorization; or
  - Where such communication is made by a business associate on behalf of the Plan and the communication is consistent with the business associate agreement.
- The Plan may not sell any PHI or otherwise receive any direct or indirect remuneration in exchange for PHI. The following circumstances are not prohibited by the Plan's policy against selling PHI or receiving direct or indirect remuneration in exchange for PHI:
  - For public health activities;
  - For research if the price charged reflects the costs of preparation and transmittal of data;
  - For treatment of an individual;
  - In connection with the sale of the company where the buyer takes over the health plan;
  - To pay a business associate for a service provided to the health plan that involves disclosing PHI; and
  - To provide someone with a copy of their own PHI.
- Any requests for the use or disclosure of PHI for fundraising or marketing purposes, or for the sale of PHI, shall be directed to the Privacy Official who shall deny such requests.

## **XXI. Disclosure of PHI to the Agency**

**OBJECTIVE:** Allow the Plan to disclose PHI to the Agency for the Agency to carry out plan administration functions that the Agency performs for the Plan, in compliance with HIPAA.

### **Procedure**

- Before the Plan discloses PHI to the Agency for plan administration functions, the Plan documents must be amended to incorporate provisions to:
  - establish the permitted and required uses and disclosures of such information by the Agency;
  - provide that the Plan will disclose PHI to the Agency only upon receipt of a certification by the Agency that the Plan has been amended to incorporate the following provisions and the Agency has agreed to:
    - not to use or further disclose PHI other than as permitted or required by the Plan or as required by law;
    - to ensure that any agents, including subcontractors, to which the Agency provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Agency;
    - not to use or disclose PHI for employment-related actions and decisions;
    - not to use or disclose PHI in connection with any other benefit or employee benefit plan of the Agency;
    - to report to the Plan any PHI use or disclosure inconsistent with the HIPAA regulations of which the Agency becomes aware;
    - to make PHI available to an individual pursuant to HIPAA's access requirements, as set forth in these Use and Disclosure Procedures;
    - to make PHI available for amendment, and incorporate any PHI amendments in accordance with HIPAA's requirements, as set forth in these Use and Disclosure Procedures;
    - to make available the information required to provide an accounting of disclosures in accordance with HIPAA, as set forth in these Use and Disclosure Procedures;
    - to make available to the Secretary of DHHS the Agency's internal practices, books and records relating to the use and disclosure of PHI

received from the Plan to determine the Plan's compliance with HIPAA's regulations;

- if feasible, to return or destroy all PHI received from the Plan that the Agency still maintains in any form, and to destroy PHI copies when they are no longer needed for the disclosure purpose. If return or destruction is not feasible, agree to limit further uses and disclosures to those purposes that make the return or destruction infeasible; and
  - to ensure that an adequate separation between the Plan and the Agency is established that describes the employees or classes of employees of the Agency that may receive PHI, that restricts access to and use by such employees to the plan administration functions that the Agency performs for the Plan, and that provides for an effective mechanism for resolving any issues of noncompliance with the Plan document.
- The Plan may:
- disclose PHI to the Agency to carry out plan administration functions that the Agency performs only consistent with these Use and Disclosure Procedures;
  - not permit a health insurance issuer or HMO with respect to the Plan to disclose PHI to the Agency, except as permitted by these Use and Disclosure Procedures;
  - not disclose and may not permit a health insurance issuer or HMO to disclose PHI to the Agency as otherwise permitted by these Use and Disclosure Procedures unless a separate statement to that effect is included in the appropriate notice of privacy practices; and
  - not disclose PHI to the Agency for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the Agency.

### **Procedures for Complying With Individual Rights**

*Individual Rights:* HIPAA gives individuals the right to access and obtain copies of their PHI 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**

**OBJECTIVE:** To facilitate compliance with HIPAA's requirement to provide individuals with access to their own PHI.

## **“Designated Record Set” Defined**

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

- the enrollment, payment, claims adjudication, and case or medical management record systems 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 (the request must be in writing).
  - 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 Official 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 Official. (Note that on receipt of requests involving claims adjudication the Agency will refer the requestor to the appropriate business associate.)***
  - Review the disclosure request to determine whether an exception to the disclosure requirement might exist. Disclosure may be denied for requests to access: (i) psychotherapy notes; (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; (iii) certain requests by inmates; (iv) information compiled during research when denial of access to the information is agreed upon; (v) information obtained under a promise of confidentiality; and (vi) other disclosures that are determined by a health care professional to be likely to cause harm. See the Privacy Official if there is any question about whether one of these exceptions applies. ***No request for access may be denied without approval from the Privacy Official.***
  - Respond to the request by providing the information or denying the request within 30 days (60 days if the information is maintained off-site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30- or 60-day period of the reasons for the extension and the date by which the Agency 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, including a description of how the individual may exercise such review rights, if applicable; and (3) a statement of how the individual may file a complaint concerning the denial to the Plan or to the Secretary of DHHS, including the name or title and telephone number of the contact person or office responsible to receive complaints. All notices of denial must be prepared or approved by the Privacy Official.
- 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 (except for inmates) 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. Note that on receipt of requests involving claims adjudication the Agency will refer the requestor to the appropriate business associate and the individual making the request may need to be directed to the business associate's office for the inspection.
- 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.
- The Agency may 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).
- If the individual has requested a review of a denial, the Plan will designate a licensed health care professional, who was not directly involved in the denial, to review the decision to deny access, and:
  - the Plan will promptly refer a request for review to such designated reviewing official;
  - the designated reviewing official will determine, within a reasonable period of time, whether or not to deny the access requested; and
  - the Plan will promptly provide written notice to the individual of the determination of the designated reviewing official.
- Disclosures must be documented in accordance with the procedure "Documentation Requirements."

- If the Plan's Privacy Official receives any request for access to an individual's information that may be maintained by the Plan's business associates, the Privacy Official will inform such business associates of the Plan's decision with respect to such request and shall cause the service provider to comply with such decision. Prior to making such a decision with regard to records held by the Plan's business associates, the Privacy Official shall consult with the affected business associates to ensure they can comply with the request, if granted. The Plan shall require its business associates to forward to the Privacy Official any requests for access that they receive directly from individuals for a decision by the Plan.

## II. Individual's Request for Amendment

OBJECTIVE: To facilitate compliance with HIPAA's requirement to provide individuals with the right to request amendments to their own PHI.

### 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 Official 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 Official. Note that on receipt of requests to amend information used in claims adjudication the Agency will refer the requestor to the appropriate business associate.***
  - 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 Official if there is any question about whether one of these exceptions applies. Contact the business associate if information used in claims adjudication is involved. ***No request for amendment may be denied without approval from the Privacy Official.***
  - 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 and whether the PHI was created by the Plan. Contact the business associate if information used in claims adjudication is involved.

- 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 Agency 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 uncorrected 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 Official. 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 to the Plan or to the Secretary of DHHS, including the name or title and telephone number of the contact person or office responsible to receive complaints.
  - 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 Agency'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.
  - Amendments must be documented in accordance with the procedure for "Documentation Requirements."
- If the Plan's Privacy Official receives any request to amend an individual's information that may be maintained by the Plan's business associates, the Privacy Official will inform such business associates of the Plan's decision with respect to such request and shall cause the service provider to comply with such decision. Prior to making such a decision with regard to records

held by the Plan's business associates, the Privacy Official shall consult with the affected business associates to ensure they can comply with the request, if granted. The Plan shall require its business associates to forward to the Privacy Official any requests for amendments that they receive directly from individuals for a decision by the Plan.

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

**OBJECTIVE:** To facilitate compliance with HIPAA's requirement to provide individuals with the right to receive an accounting of certain disclosures of their PHI.

#### **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 provide 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 Plan will respond.
  - The accounting must include disclosures (but not uses) of the requesting individual's PHI made by the Plan and any of its business associates during the period requested by the individual up to 6 years prior to the request. (Note, however, that the plan is not required to account for any disclosures made prior to January 1, 2006.) 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;
  - to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
  - 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.
- Contact the third party claims administrator's and the pharmacy benefits manager's client services departments to obtain a listing of disclosures they have made within the past 6 years (or since the last accounting, if more recently).
  - The accounting must include the following information for each 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 Official for more guidance.
  - Accountings must be documented in accordance with the procedure for "Documentation Requirements."
  - If the Plan's Privacy Official receives any request for an accounting of disclosures of an individual's information that may be maintained by the Plan's business associates, the Privacy Official will inform such business

associates of the Plan's decision with respect to such request and shall cause the service provider to comply with such decision. Prior to making such a decision with regard to records held by the Plan's business associates, the Privacy Official shall consult with the affected business associates to ensure they can comply with the request, if granted. The Plan shall require its business associates to forward to the Privacy Official any requests for an accounting of disclosures that they receive directly from individuals for a decision by the Plan.

#### **IV. Processing Requests for Confidential Communications**

**OBJECTIVE:** Facilitate processing of 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 (the request must be in writing).
  - 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 that provide an alternate address and a reasonable basis for the request (for example, an impending divorce). Requests for confidential communications must be honored by the Plan if the individual states that disclosure could endanger the individual.
  - 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 noted in the member's file within 3 working days, with the alternate address entered for the requesting party in the same manner that an alternate address is noted for a COBRA participant.
  - Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

- If the Plan's Privacy Official receives any request for confidential communications of an individual's information that may be maintained by the Plan's business associates, the Privacy Official will inform such business associates of the Plan's decision with respect to such request and shall cause the service provider to comply with such decision. Prior to making such a decision with regard to records held by the Plan's business associates, the Privacy Official shall consult with the affected business associates to ensure they can comply with the request, if granted. The Plan shall require its business associates to forward to the Privacy Official any requests for confidential communications that they receive directly from individuals for a decision by the Plan.

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

**OBJECTIVE:** To facilitate the processing of requests for restrictions on uses and disclosures of PHI.

- *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 restriction 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 only if the requesting party provides a compelling reason to honor the request (such as endangerment of the individual's well-being should the information be released).
  - The Plan is only required by law to agree with a request in the case of a request to restrict a disclosure to a health plan for purposes of carrying out payment or health care operations (and not for purposes of carrying out treatment), provided the PHI pertains solely to a health care item or service for which a health care provider involved has been paid out of pocket in full. In all other cases, the Plan is not required by law to agree with a request for a restriction.
  - 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 noted in the member's folder.

- All business associates that may have access to the individual's PHI must be notified of any agreed-to restrictions. The staff of the Senior Advisor Retiree Health Care shall contact the client services department of the business associate(s) and advise them of the agreement to restrict access.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."
- Even if the Plan has agreed to a restriction, the Plan may continue to use and disclose PHI as follows:
  - to the individual whose PHI is being restricted;
  - as required by law;
  - for the purposes described in these Use and Disclosure Procedures related to public policy uses and disclosures; or
  - to the Secretary of the Department of Health and Human Services to investigate or determine the Plan's compliance with the Privacy Regulations.
- The Plan may terminate its agreement to a restriction, if:
  - the individual agrees to or requests the termination in writing;
  - the individual orally agrees to the termination and the oral agreement is documented; or
  - except for a restriction request that is required by law to be honored, the Plan informs the individual that the Plan is terminating the agreement, except that such termination is only effective with respect to PHI created or received after it has so informed the individual.
- The Privacy Official shall document the termination of a restriction and shall retain that documentation for a period of at least 7 years from the date of its creation.
- If the Plan's Privacy Official receives any request for restrictions as to the use or disclosure of information that may be maintained by the Plan's business associates, the Privacy Official will inform such business associates of the Plan's decision with respect to such request and shall cause the service provider to comply with such decision. Prior to making such a decision with regard to records held by the Plan's business associates, the Privacy Official shall consult with the affected business associates to ensure they can comply with the request, if granted. The Plan shall require its business associates to forward to the Privacy Official

any requests for restrictions that they receive directly from individuals for a decision by the Plan.

## VI. Notice of Privacy Practices, Complaints, and Privacy Official

**OBJECTIVE:** Comply with HIPAA's requirements to: (1) provide individuals with the right to notice of the Plan's uses and disclosures of their PHI, their individual rights, and the Plan's legal duties with respect to PHI; (2) provide a means for individuals to lodge complaints about the Plan's uses and disclosures of their PHI; and (3) appoint a Privacy Official to serve as the individual charged with leading and managing the implementation of these Use and Disclosure Procedures.

### Procedure

- Timing of Notice.* The Plan will provide its Notice of Privacy Practices ("Notice"):
  - at the time of enrollment, to individuals who are new enrollees; and
  - within 60 days of a material revision to the Notice, to individuals then covered by the Plan.
- New Enrollees.* New enrollees will receive the Notice in their initial enrollment package, along with their summary plan description booklet and other initial notices.
- Updates.* No less frequently than once every three years, the Plan will notify individuals then covered by the Plan of the availability of the Notice and how to obtain the Notice.
- One Notice Per Family.* The Plan will provide the Notice to the employee who is enrolled in the Plan and will not provide a separate notice to any dependents of the employees who are also covered by the Plan, unless a Notice is specifically requested by any such dependent.
- Single Notice For All Coverage Options.* The Plan will provide the same Notice to all participants, regardless of which benefit program or coverage level in which the participant is enrolled.
- Web Site.* If the Agency maintains a web site that provides information about the Plan's benefits, it will prominently post the Plan's Notice on that web site and make the Notice available electronically through the web site.
- Complaints.* Any individual who believes that his or her privacy rights have been violated may lodge a complaint with the Plan's Privacy Official who will investigate and respond to all complaints filed. The Plan's Notice of Privacy Practices will notify individuals of this right, as well as the right to file a

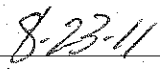
complaint with the Secretary of DHHS. The Privacy Official shall document all steps involved in the investigation (including, but not limited to, the individual's original complaint) and shall retain such documentation for at least 6 years after the complaint is fully resolved.

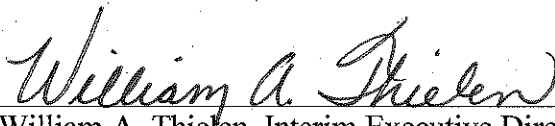
- *Documentation.* The Plan will document compliance with the notice requirements, by retaining copies of the Notice issued by the Plan for 6 years from the date of the Notice's creation or the date when it was last in effect, whichever is later.
- *Business Associates.* The Privacy Official shall ensure that each business associate of the Plan has a current copy of the Plan's Notice and, through the business associate contract, agrees to use and disclose PHI and to implement individuals' right with respect to their PHI consistently with the Notice.
- *Privacy Official.* The Privacy Official shall be appointed by the Agency in its role as administrator of the Plan. The Privacy Official will coordinate the implementation of these Use and Disclosure Procedures. The Privacy Official will implement, manage, regularly monitor, and maintain compliance with these Use and Disclosure Procedures and the requirements of the HIPAA regulations. The Privacy Official shall have all duties set forth in these Use and Disclosure Procedures and shall serve at the pleasure of the Agency.

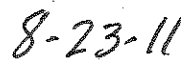
#### CERTIFICATION

We, the Chair of the Board of Trustees and the Executive Director, do hereby certify that this HIPAA Privacy Use and Disclosure Procedures Kentucky Retirement Systems was amended by the Board of Trustees on this the 18th day of August, 2011.

  
\_\_\_\_\_  
Jennifer L. Elliott, Chair

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
William A. Thielen, Interim Executive Director

  
\_\_\_\_\_  
Date