

# **MUNICIPAL EMPLOYEES' RETIREMENT SYSTEM OF MICHIGAN HEALTH CARE SAVING PROGRAM**

---

## **HIPAA PRIVACY POLICIES AND PROCEDURES**

---

**Revised:** October 1, 2018

Terms used, but not otherwise defined, in these Policies and Procedures have the meanings set forth in the Glossary located at the end of this document and 45 C.F.R. Parts 160, 162, and 164 ("Privacy Regulations"). All references to the "Plan" refer to the Health Care Savings Program and any other health plans or programs providing medical care benefits (including health, dental, vision, long term care, or other coverage affecting any structure of the body) that are sponsored by Municipal Employees' Retirement System of Michigan and that are subject to the Privacy Regulations and are either (i) uninsured, or (ii) insured and provide PHI to Municipal Employees' Retirement System of Michigan. The Plan reserves the right to change these Policies and Procedures at any time.

# TABLE OF CONTENTS

	Page
Introduction.....	1
Policy and Procedure On Uses and Disclosures .....	2
Without Consent .....	2
Policy and Procedure on Written Authorizations .....	3
Policy and Procedure on Disclosures to Spouses, Family, and Others (Verbal Agreements).....	6
Policy and Procedure for Personal Representatives, Dependent Children, and Deceased Individuals.....	8
Policy and Procedure on Public Policy Uses and Disclosures.....	10
Policy and Procedure on Disclosure of PHI to Plan Sponsor .....	12
Policy and Procedure on Disclosures to Business Associates .....	14
Policy and Procedure for Limited Data Set .....	17
Policy and Procedure for Minimum Necessary Requirement.....	19
Policy and Procedure for Verification of Individual's Identity and Authority .....	21
Policy and Procedure for De-Identification .....	23
Policy and Procedure for Notice of Privacy Practices, Complaints, and Privacy Officer .....	25
Policy and Procedure for an Individual's Right to Request Restrictions .....	28
Policy and Procedure for an Individual's Right to Request Confidential Communications .....	30
Policy and Procedure for an Individual's Right to Request to Inspect and Obtain A Copy of PHI.....	32
Policy and Procedure for an Individual's Right to Request an Amendment to PHI .....	35
Policy and Procedure for an Individual's Right to Request an Accounting of Disclosures .....	38
Policy and Procedure for Securing PHI and Notification in Case of Breach of Unsecured PHI ..	41
Policy and Procedure for Employee Education and Discipline .....	46
Policy and Procedure For Administrative, Physical, And Technical Safeguards For PHI.....	47
Glossary.....	50

## **INTRODUCTION**

The Municipal Employees' Retirement System of Michigan (MERS) established and maintains the Health Care Savings Program (HCSP), which is a post-employment/retiree-only health reimbursement plan. As such, many of the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), while legally applicable to MERS, have limited or no practical applicability to any activity in which the MERS' HCSP engages. For example, the HCSP engages in no treatment activities, and it receives no genetic information. Therefore, those requirements of the HIPAA Privacy and Security Rule with no applicability to the MERS HCSP have been removed from these Policies and Procedures to avoid confusion or misrepresentation; at any time, should any of these become or be anticipated to apply to the MERS HCSP, it/they shall be deemed included retroactively to such time, and the Policies/Procedures revised to so reflect as soon as administratively feasible.

## POLICY AND PROCEDURE ON USES AND DISCLOSURES WITHOUT CONSENT

### **Purpose**

The Privacy Regulations allow the Plan to use or disclose PHI for Treatment activities, Payment activities, and Health Care Operations without the explicit written consent of an individual. However, the Privacy Regulations allow for the Plan to obtain such a consent if it chooses to do so.

### **Policy**

The Plan will use or disclose PHI for Payment activities and Health Care Operations *without obtaining the written consent of the individual* as allowed under applicable law, for the following uses and disclosures:

1. for the Plan's own Payment activities or Health Care Operations; or
2. to another Health Plan, Health Care Clearinghouse, or Health Care Provider for Payment activities of the entity that receives the information.

### **Procedure**

1. No Consent Necessary. No special procedures are required to use or disclose PHI for the purposes identified above. These uses and disclosures are subject to the Plan's Policies and Procedures and in particular, the Plan's Policy and Procedure for the Minimum Necessary Requirement (page 19) and for Verification of Individual's Identity and Authority (page 21).
2. Inquiries. Any questions regarding whether a particular use or disclosure of PHI is permissible under this Policy should be directed to the Plan's Privacy Officer. In the Privacy Officer's absence, such questions may be directed to legal counsel.
3. Cross-References. If a particular use or disclosure is not authorized by this Policy, the PHI may not be used or disclosed unless allowed by one of the following policies:
  - (a) Policy and Procedure on Written Authorizations (page 3);
  - (b) Policy and Procedure on Disclosures to Spouses, Family, and Others (Verbal Agreements) (page 6);
  - (c) Policy and Procedure on Public Policy Uses and Disclosures (page 10);
  - (d) Policy and Procedure on Disclosures to Business Associates (page 14);
  - (e) Policy and Procedure for Limited Data Set (page 17);
  - (f) Policy and Procedure for De-Identification (page 23); and
  - (g) Policy and Procedure on Disclosures of PHI to Plan Sponsor (page 12); and
  - (h) Policy and Procedure for an Individual's Right to Request to Inspect and Obtain a Copy of PHI (page 32).

## **POLICY AND PROCEDURE ON WRITTEN AUTHORIZATIONS**

### **Purpose**

Except as otherwise allowed by the Privacy Regulations or these Policies and Procedures, the Plan will not use and disclose PHI about an individual without a written authorization. This Policy and Procedure governs when the Plan will obtain an authorization and the form of the authorization.

### **Policy**

1. The Plan will require an authorization to use or disclose PHI if that use or disclosure of PHI is not otherwise permitted by the Privacy Regulations or these Policies and Procedures without an authorization.
2. The Plan may use or disclose PHI without an authorization for the following purposes:
  - (a) For Payment activities, or Health Care Operations (as set forth in the Policy and Procedure on Uses and Disclosures without Consent, page 1);
  - (b) Pursuant to an agreement with an individual (as set forth in the Policy and Procedure on Disclosures to Spouses, Family, and Others (Verbal Agreements), page 6);
  - (c) For any "public policy" purpose (identified in the Policy and Procedure on Public Policy Uses and Disclosures, page 10); or
  - (d) As Required By Law.
3. Any authorization form required by this Policy must comply with the requirements set forth in the Procedures section below.
4. Any use or disclosure of PHI requiring an authorization will be made only with the approval of the Plan's Third-Party Administrator ("TPA") or Privacy Officer.

### **Procedure**

1. General Authorization Forms. If the Plan needs to use or disclose PHI for any purpose that is not identified in item 2 above, a written authorization must first be obtained from the individual. **Form 7 (Authorization Form)** may be used for this purpose. In addition, any form adopted by the Plan's TPA may constitute a valid authorization if it contains the elements in paragraphs 3 and 4 below.
2. Review and Approval of Authorization. The Plan's Privacy Officer or TPA will review all completed authorization forms prior to any disclosure to make sure it contains the following required elements:
  - (a) A specific description of the information to be used and disclosed;
  - (b) The name or specific identification of the person or class of persons authorized to use the information or make the disclosure;
  - (c) The name or specific identification of the person or class of persons to whom the Plan may make the requested disclosure;
  - (d) A description of each purpose of the requested use or disclosure (the statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose);
  - (e) An expiration date or event that relates to the individual or the purpose of the use or disclosure; and

- (f) The signature of the individual, the signature date, and if the authorization is signed by a personal representative of the individual, a description of the representative's authority to act on behalf of the individual.

The Plan's TPA, Privacy Officer or other staff may complete the required elements described above prior to obtaining the individual's signature on the authorization form; however, the individual must personally sign the authorization.

3. Required Provisions. The Plan's authorization form contains certain required provisions placing the individual on notice of each of his or her rights. If the Privacy Officer or TPA receives an authorization form that was not created by the Plan, prior to disclosing information pursuant to such form, the TPA or Privacy Officer will verify that that form contains the required elements in item 3 as well as the following rights:
  - (a) 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).
  - (b) The ability of the Plan to condition Payment, enrollment, or eligibility for benefits on the authorization by stating either:
    - (i) The Plan may not condition Payment, enrollment, or eligibility for benefits on whether the individual signs the authorization; or
    - (ii) 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 (see paragraph 5 below for times when the Plan may impose conditions).
  - (c) 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.
4. When Authorization May Be Required by the Plan. The Plan will not condition Payment, enrollment, or eligibility for benefits upon an individual's signing an authorization, except the Plan may condition enrollment in the Plan's programs, or eligibility for benefits, on the provision of an authorization requested by the Plan prior to an individual's enrollment if that authorization is for the purpose of the Plan's eligibility or enrollment decisions relating to the individual or the Plan's underwriting or risk rating (so long as the authorization does not apply to Psychotherapy Notes).
5. Revoking Authorizations. The Plan and the TPA 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.
6. Retention. The Plan will retain any signed authorization forms for six years from the later of the date they were created or last in effect. The Plan will require the TPA to retain authorization forms in compliance with this paragraph.
7. Invalid Authorizations. The Privacy Officer or the TPA will not approve any disclosures pursuant to an invalid authorization. An authorization is invalid if it contains any of the following defects:
  - (a) The expiration date has passed (or if it expires upon an event, the Plan knows the event has passed);
  - (b) The authorization has not been filled out completely;
  - (c) The Plan knows the authorization has been revoked;

- (d) The authorization conditions the Payment, enrollment in the Plan, or eligibility for benefits upon providing the authorization;
  - (e) The Plan knows any material information in the authorization is false.
8. Compound Authorizations. An authorization for the use or disclosure of PHI may not be combined with any other document to create a compound authorization.
  9. Copies to Individuals. If the Plan has requested the authorization from an individual for its own purposes, the Plan will provide the individual with a copy of the signed authorization. In all other instances, the Plan will provide the individual with a copy of the signed authorization upon request.
  10. Disclosures to Spouses and Parents. The Plan recognizes that spouses and parents sometimes seek the disclosure of their spouse's and non-minor dependent's PHI for purposes of tracking health claims and resolving claims disputes. If the Plan is unable to disclose PHI to a spouse or parent after applying the criteria set forth in Policy and Procedure on Disclosures to Spouses, Family, and Others (Verbal Agreements) (page 6), the Plan will require an authorization from the spouse or non-minor dependent whose PHI is to be disclosed. **Form 7 (Authorization for Use and Disclosure of Protected Health Information)**. Notwithstanding this provision, limited information related to claims status and payment history may be disclosed to the employee who is the primary enrollee in the Plan without such an authorization, provided that such information does not include any information related to the health services associated with the claim.

## **POLICY AND PROCEDURE ON DISCLOSURES TO SPOUSES, FAMILY, AND OTHERS** **(VERBAL AGREEMENTS)**

### **Purpose**

The Privacy Regulations allow the Plan to use and disclose PHI for purposes of making disclosures to people involved in an individual's care, and for notification purposes, provided that, except in emergency situations, such uses or disclosures are consistent with the individual's agreement or the individual's failure to object after being given an opportunity to do so.

### **Policy**

1. The Plan will not disclose an individual's PHI to the individual's spouse or any other person involved in the individual's care, unless the PHI is directly relevant to such person's involvement with the individual's care or Payment related to the individual's care.
2. The Plan will generally not disclose an individual's PHI to people involved in an individual's care or the Payment for that care unless the Plan first obtains a written authorization form from the individual whose PHI is to be disclosed. However, in emergency situations, under other circumstances approved by the Privacy Officer, or as otherwise provided in this Procedure, the Plan may disclose PHI to people involved in an individual's care or Payment for care if the Plan first:
  - (a) Informs the individual of the request and provides the individual with an opportunity to object to the disclosure; or
  - (b) If the individual is not available, is incapacitated, or if an emergency exists, in the exercise of professional judgment, determines that the disclosure is in the individual's best interest.
3. The Plan may use or disclose PHI to notify, or assist in the notification of (including identifying or locating) a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death, if the Plan first:
  - (a) Informs the individual of the request and provides the individual with an opportunity to object to the disclosure; or
  - (b) If the individual is not available, is incapacitated, or if an emergency exists, in the exercise of professional judgment, determines that the disclosure is in the individual's best interest.
  - (c) If the individual is deceased, in the exercise of professional judgment, determines that the disclosure is in the individual's best interest and is not inconsistent with any prior expressed preference of the individual known to the Plan.
4. This Policy will apply to disclosures to spouses, as well as disclosures to parents of dependents age 18 and older, but will not apply to dependents under the age of 18. Refer to the Policy and Procedure on Personal Representatives and Dependent Children (page 8) for special rules that will apply to dependents under age 18.

### **Procedure**

1. Spouses, Family Members and Others. If the Plan receives a request to disclose an individual's PHI to that individual's spouse or parent (if the individual is a non-minor dependent) and the individual is not present, the Plan may disclose the PHI if, in the discretion of a Workforce member of the Plan or an authorized representative of the TPA, if the standards of paragraph 4 are met. In addition, the Plan may release limited claims related information about spouses and

non-minor dependents to the Plan's primary enrollee so that the primary enrollee can monitor the proper payment of the claims of the enrollee and his or her dependents. In either case, disclosures shall be limited to the minimum necessary amount of information needed for this purpose in accordance with the Policy and Procedure for Minimum Necessary Requirement (page 19). Any other request of an individual's PHI by an individuals' family member, other relative, or close personal friend will generally require a written authorization from the individual whose PHI is to be disclosed. Such authorization shall comply with the requirements of the Policy and Procedure on Written Authorization (pages 3 and 5).

2. Notification. The Plan may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Before the Plan makes such a use or disclosure, the Privacy Officer shall inform the individual of the use or disclosure and provide the individual with an opportunity to object to the use or disclosure. If the individual is not available or is incapacitated, or if any emergency exists, the Privacy Officer may, in the exercise of professional judgment, determine that the disclosure is in the individual's best interest.
3. Disaster Relief. The Plan may disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph 2 above. The Plan (through the Privacy Officer) will provide individuals with an opportunity to object to such disclosures, unless doing so would interfere with the Plan's or other entity's need to respond to the emergency circumstance.
4. Individual Not Present/Incapacitated. If the Plan cannot provide the individual with an opportunity to object because the individual is not present, is incapacitated, or there is an emergency situation, any request for a disclosure of the individual PHI will be handled by the Plan's TPA or the Privacy Officer (or the Privacy Officer's designee). The TPA or the Privacy Officer (or the Privacy Officer's designee) may proceed with limited, relevant disclosures to a spouse or parent (if the individual is a non-minor dependent) involved in the individual's care or the Payment for the individual's care if the TPA or the Privacy Officer reasonably infers from the circumstances, based on the exercise of professional judgment, that the disclosure would be in the individual's best interests.
5. Deceased Individual. The Plan may disclose an individual's PHI in the case of death to a family member, relative, or close personal friend involved in the health care or Payment for health care of the individual prior to death. The TPA or the Privacy Officer may proceed with disclosures limited to the person's involvement in the health care or Payment for health care of the individual prior to the individual's death if the TPA or the Privacy Officer reasonably infers from the circumstances, based on the exercise of professional judgment, that the disclosure would be in the individual's best interests unless Plan's TPA or the Privacy Officer determines doing so is inconsistent with any prior express preference of the individual that is known to the Plan. Information is no longer considered PHI once an individual has been deceased for 50 years.

## **POLICY AND PROCEDURE FOR PERSONAL REPRESENTATIVES, DEPENDENT CHILDREN, AND DECEASED INDIVIDUALS**

### **Purpose**

The Privacy Regulations provide that if a person has authority to act on behalf of an individual who is an adult, an emancipated minor, an unemancipated minor, or deceased in making decisions related to health care, the Plan should treat such person as a personal representative, with respect to PHI relevant to such personal representation. Thus, a personal representative generally may receive and direct the use and disclosure of another individual's PHI and exercise that person's rights with respect to the PHI.

### **Policy**

General Rules. The Plan will recognize the authority of the following individuals to act on behalf of themselves or others with respect to PHI and will treat them as "personal representatives" of individuals under the Plan:

1. Adults and Dependents Age 18 and Over. The Plan will presume that all adults and all dependents age 18 and over have the authority to act on their own behalf with respect to their own PHI unless the Plan receives legal documentation indicating otherwise.
2. Parents, Guardians, and Persons Acting *in loco parentis*. Except as set forth below, the Plan will presume that all parents, whether custodial or non-custodial, have the authority to act on behalf of their dependents who are under the age of 18. The Plan will require legal documentation that an individual is serving as the minor's guardian or in some other legal capacity for the minor before the Plan will treat the individual as the minor's parent. Step-parents will not be treated as parents for purposes of this rule without the written authorization of one of the minor's parents.
3. Dependents Under Age 18. The Plan will allow dependents under age 18 to act on their own behalf in limited circumstances noted below.
4. Personal Representatives. Except as set forth below, the Plan will recognize the authority of any personal representative of an individual or deceased individual to act on behalf of such individual or deceased individual upon receipt of the appropriate legal documentation reflecting the personal representative's authority, such as a power of attorney, a guardianship order, or an order appointing an individual as an executor or administrator of an estate.

### **Procedure**

1. Verification of Identity and Authority. For any request to disclose information to a parent, guardian, or personal representative, the Plan will first verify the identity and authority of the individual making the request according to the Plan's Policy and Procedure for Verification of Individual's Identity and Authority (page 21).
2. Special Circumstances. After verifying the individual's identity and authority, the Plan will make sure that it is appropriate to treat the individual as the parent, guardian, or personal representative in the following circumstances:
  - (a) Personal Representatives for Dependents Under Age 18. The Plan will not treat a person as the personal representative of an unemancipated minor if:
    - (i) the PHI sought relates to a matter for which the minor has authority to act on his or her own behalf under state law, or a matter for which a parent's or other guardian's consent is not needed,

- (ii) the PHI relates to medical treatment that was provided to the minor under confidential circumstances and the Plan is made aware of such confidential circumstances, or
    - (iii) the parent or guardian agrees to an agreement of confidentiality between a Health Care Provider and the minor regarding a health care service and the Plan is made aware of such agreement.
  - (b) Personal Representatives for Any Individual (Including Dependents Under Age 18). The Plan may elect not to treat a person as the personal representative of an individual if:
    - (i) the Plan has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
    - (ii) treating such person as the personal representative could endanger the individual; and
    - (iii) the Plan's TPA or the Privacy Officer, in the exercise of professional judgment, decides that it is not in the best interests of the individual to treat the person as the individual's personal representative.
- 3. Deceased Individual. The Plan may disclose a deceased individual's PHI to an executor, administrator, or other person who has the authority to act on behalf of a deceased individual or on behalf of the deceased individual's estate. Information is no longer considered PHI once an individual has been deceased for 50 years.
- 4. Confidential Communications. Any individual may request that the Plan not treat another person as his or her personal representative by completing **Form 3 (Request for Confidential Communications)** and submitting it to the Plan's TPA or the Privacy Officer.

## **POLICY AND PROCEDURE ON PUBLIC POLICY USES AND DISCLOSURES**

### **Purpose**

The Privacy Regulations allow for the Plan to use or disclose PHI without obtaining the individual's authorization when such use or disclosure serves a public policy identified and described in this Policy and Procedure.

### **Policy**

1. **Permitted.** The Plan will use and disclose PHI without obtaining the individual's authorization for certain public policy reasons as allowed in the Privacy Regulations and set forth below:
  - (a) As Required By Law; or
  - (b) In the course of a judicial or administrative proceeding in response to any court or administrative order (including, but not limited to a qualified medical child support order).

### **Procedure**

1. **Legal Orders and Similar Requests.** Upon receipt of any court or administrative order, subpoena, discovery request, or other legal process requiring the disclosure of PHI, the Plan will forward the request to legal counsel for legal review prior to making any disclosure.
  - (a) **Court and Administrative Orders.** Legal counsel will verify the validity of the order and advise the Plan as to whether the requested disclosure may be made. If the order is valid, legal counsel will advise the Privacy Officer who shall authorize the disclosure of only the PHI that is expressly sought by the order. If the order is not valid, the Plan (through legal counsel after consulting with the Privacy Officer) shall take reasonable and appropriate steps to notify the court or administrative body that issued the order of the Plan's objections to releasing the PHI.
  - (b) **Subpoenas, Discovery, and Other Legal Process.** Legal counsel will verify the validity of the request and 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 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 in 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 PHI has made reasonable efforts to secure 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.

All of the foregoing information under either (i) or (ii) must be provided to the Plan by the party seeking the disclosure. Neither the Plan, nor its legal counsel, shall have any obligation to independently seek an individual's authorization to a disclosure sought by a

subpoena, discovery request, or other legal process, or to secure or request a qualified protective order.

2. Legal Orders and Similar Requests Received by Service Provider. The Privacy Officer, by contract or otherwise, may require a service provider (such as the Plan's TPA or TPA's subcontractor), to notify the Plan upon receipt of any court or administrative order, subpoena, discovery request, or other legal process requiring the disclosure of PHI maintained by such service provider on behalf of the Plan. Upon receiving such notice, the Plan may, after consulting with legal counsel, choose to respond to the subpoena, object to the subpoena, or to otherwise intervene in the action to which the subpoena pertains.
3. Other Disclosures Required By Law. Upon receipt of any request for the Plan to disclose PHI for any other public policy purposes, or upon receipt of any request for the Plan to disclose PHI due to any legal requirement, the Plan will forward the request to legal counsel for legal review prior to making the disclosure.
4. Logging Disclosures. All disclosures made pursuant to this Policy must be reported to the Plan's Privacy Officer who will log the disclosure.

## **POLICY AND PROCEDURE ON DISCLOSURE OF PHI TO PLAN SPONSOR**

### **Purpose**

The Privacy Regulations allow the Plan to disclose PHI to the Plan Sponsor for the Plan Sponsor to carry out plan administration functions that the Plan Sponsor performs for the Plan if certain protective steps are implemented. The Plan will allow these disclosures consistent with this Policy and Procedure.

### **Policy**

1. The Plan will disclose an individual's PHI to the Plan Sponsor to carry out plan administration functions that it performs for the Plan. For these purposes, "plan administration functions" means administrative functions performed by the Plan Sponsor on behalf of the Plan and excludes functions performed by the Plan Sponsor in connection with any other benefit or benefit plan of the Plan Sponsor, or in the Plan Sponsor's role as an employer.
2. Before the Plan discloses PHI to the Plan Sponsor, the Plan will follow the procedures set forth below.

### **Procedure**

1. Requirements for Disclosure to Plan Sponsor. If the Plan receives a request to disclose an individual's PHI to the Plan Sponsor, the Plan will ensure that the Plan document has been amended as provided in paragraph 2 below.
2. Plan Amendments. Before the Plan discloses PHI to the Plan Sponsor for plan administration functions, the Plan document must be amended to incorporate provisions to:
  - (a) establish the permitted and required uses and disclosures of such information by the Plan Sponsor;
  - (b) provide that the Plan will disclose PHI to the Plan Sponsor only upon receipt of a certification by the Plan Sponsor that the Plan has been amended to incorporate the following provisions and the Plan Sponsor has agreed to:
    - (i) not to use or further disclose Protected Health Information other than as permitted or required by the Plan or as Required By Law;
    - (ii) to ensure that any agents, including subcontractors, to which the Plan Sponsor provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor;
    - (iii) not to use or disclose PHI for employment-related actions and decisions;
    - (iv) not to use or disclose PHI in connection with any other benefit or employee benefit plan of the Plan Sponsor;
    - (v) to report to the Plan any PHI use or disclosure inconsistent with the Privacy Regulations' requirements of which the Plan Sponsor becomes aware;
    - (vi) to make PHI available to an individual pursuant to the Privacy Regulations' access requirements at 45 CFR § 164.524;
    - (vii) to make PHI available for amendment, and incorporate any PHI amendments in accordance with the Privacy Regulations at 45 CFR § 164.526;
    - (viii) to make available the information required to provide an accounting of disclosures in accordance with the Privacy Regulations at 45 CFR § 164.528;
    - (ix) to make available to the Secretary of the Department of Health and Human Services the Plan Sponsor'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 the Privacy Regulations;

- (x) if feasible, to return or destroy all PHI received from the Plan that the Plan Sponsor 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
- (xi) to ensure that an adequate separation between the Plan and the Plan Sponsor is established that describes the employees or classes of employees of the Plan Sponsor that may receive PHI, that restricts access to and use by such employees to the plan administration functions that the Plan Sponsor performs for the Plan, and that provides for an effective mechanism for resolving any issues of noncompliance with the Plan document.

3. Uses and Disclosures. The Plan may:

- (a) disclose PHI to the Plan Sponsor to carry out plan administration functions that the Plan Sponsor performs only consistent with this Policy and Procedure;
- (b) not disclose PHI to the Plan Sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor.

## **POLICY AND PROCEDURE ON DISCLOSURES TO BUSINESS ASSOCIATES**

### **Purpose**

The Privacy Regulations allow the Plan to disclose PHI to its Business Associates and to allow its Business Associates to create, receive, maintain, or transmit PHI on the Plan's behalf, if the Plan first obtains satisfactory assurance that the Business Associate will appropriately safeguard the information.

### **Policy**

1. The Plan will identify those Business Associates that create, receive, maintain, or transmit PHI of Plan participants and beneficiaries in order to perform services for the Plan.
2. The Plan will ensure that it obtains satisfactory assurance that its Business Associates will appropriately safeguard PHI disclosed to, or created by or received by, its Business Associates. Such satisfactory assurance shall be in the form of a written contract.
3. This Policy will not apply to certain disclosures by the Plan to the Plan Sponsor as allowed under the Privacy Regulations.
4. For this purpose, "Business Associate" has the meaning set forth in the Glossary, but generally means a person who, on behalf of the Plan:
  - (a) creates, receives, maintains, or transmits Protected Health Information for a function or activity regulated by the Privacy Regulations; or
  - (b) provides legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services to or for the Plan where the provision of the service involves the disclosure of PHI from the Plan.

### **Procedure**

1. Identification of Business Associates. The Plan's Privacy Officer will identify all potential Business Associates of the Plan, and will send a "Business Associate contract" to each Business Associate identified and oversee the execution and timely return of those contracts. In the alternative, the Plan may execute a Business Associate contract provided to the Plan by the Business Associate, provided however that the Plan's Privacy Officer will first ensure that the contract complies with paragraph 4 below.
2. Subcontractors of Business Associates. The Plan is not required to obtain agreements with subcontractors of the Plan's Business Associates. The Plan's Business Associates shall be required to obtain satisfactory assurance that its subcontractors will appropriately safeguard PHI disclosed to, or created by or received by, its subcontractors. Such satisfactory assurance shall be in the form of a written contract.
3. Effect of No Agreement. The Plan's Privacy Officer will advise Workforce members and others who perform any service on behalf of the Plan as to any identified Business Associates who have not executed and returned the Business Associate contract, and employees and service providers will not disclose PHI to any entity who has been identified as a Business Associate if that entity has not returned an executed Business Associate contract to the Plan.
4. Contents of Agreements. The Plan's Business Associate contracts will, at a minimum:
  - (a) establish the permitted and required uses and disclosures of PHI by the Business Associate;

- (b) permit the Business Associate to provide Data Aggregation services relating to the Health Care Operations of the Plan; and
- (c) require the Business Associate to:
  - (i) 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;
  - (ii) use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by its contract;
  - (iii) comply with the security and privacy provisions made directly applicable to Business Associates under the HITECH Act, including with respect to electronic PHI;
  - (iv) report to the Plan any use or disclosure of the PHI not provided for under the contract, including Breaches of Unsecured PHI (see Policy and Procedure for Securing PHI and Notification in Case of Breach of Unsecured PHI, page 42);
  - (v) ensure that any agents or subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate on behalf of the Plan agree to and maintain a Business Associate agreement containing the same restrictions and conditions that apply to the Business Associate with respect to such information;
  - (vi) make available PHI so that the Plan can satisfy its access, amendment, and accounting obligations to individuals;
  - (vii) to the extent the Business Associate is to carry out the Plan's obligations under the Privacy Regulations, comply with the requirements of the Privacy Regulations that apply to the Plan in the performance of such obligations;
  - (viii) 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 the Privacy Regulations;
  - (ix) 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
  - (x) authorize termination of the contract and any other agreement with the Business Associate by the Plan, if the Plan determines that the Business Associate has violated a material term of the contract.

The Privacy Officer shall have the authority to propose other requirements to a Business Associate or to agree to other terms that are not inconsistent with this paragraph such as requiring indemnification from a Business Associate in the event its acts result in liability for the Plan. Business Associate agreements may also permit the Business Associate to use PHI for the proper management and administration of the Business Associate or to carry out the Business Associate's legal responsibilities. The Business Associate agreement may also permit the Business Associate to disclose PHI for the Business Associate's proper management and administration functions, or for the legal responsibilities of the Business Associates if: (a) the disclosure is Required By Law; or (b) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

5. Violations of Agreements. The Plan's Privacy Officer will ensure, to the best of his or her ability, that the Business Associate takes steps to cure any breach of the agreement or any violation of the

rules. If cure is not possible, the Privacy Officer shall terminate the Business Associate agreement and any underlying agreement or relationship with the Business Associate, if feasible.

6. Documentation. The Privacy Officer shall maintain copies of each Business Associate contract for at least six years after the contract's final term ends.

## **POLICY AND PROCEDURE FOR LIMITED DATA SET**

### **Purpose**

The Privacy Regulations allow the Plan to use or disclose a limited data set for research, public health activities, or Health Care Operations purposes without authorization from the individual whose PHI is used.

### **Policy**

1. The Plan may use or disclose a limited data set for purposes of research, public health activities, or Health Care Operations, if the Plan enters into a data use agreement with the limited data set recipient.
2. The Plan may use PHI to create a limited data set or disclose PHI to a Business Associate for such purpose, whether or not the limited data set is to be used by the Plan.

### **Procedure**

1. Identification of Need for Data Use Agreements. The Plan's Privacy Officer will identify any potential need for use of a limited data set and any potential limited data set recipients, and will send a "data use agreement" to each limited data set recipient identified and oversee the execution and timely return of those contracts. Limited data sets may only be used for research, public health, or Health Care Operations.
2. Effect of No Agreement. The Plan's Privacy Officer will advise Workforce members and others who perform services on behalf of the Plan as to any identified limited data set recipient who has not executed and returned the requested agreement, and employees or service providers will not disclose a limited data set to any entity who has been identified as a limited data set recipient if that entity has not returned an executed data use agreement to the Plan.
3. Contents of Agreement. A data use agreement between the Plan and the limited data set recipient will:
  - (a) establish the permitted uses and disclosures of such information by the limited data set recipient;
  - (b) not authorize the limited data set recipient to use or further disclose the information in a manner that would be a violation of the Privacy Regulations, if done so by the Plan;
  - (c) establish who is permitted to use or receive the limited data set; and
  - (d) provide that the limited data set recipient will:
    - (i) not use or further disclose the information other than as permitted by the data use agreement or as otherwise Required By Law;
    - (ii) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
    - (iii) report to the Plan any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
    - (iv) ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
    - (v) not identify the information or contact the individuals to whom the information pertains.
4. Privacy Officer Role. Any data use agreement must be approved by the Plan's Privacy Officer and may only be executed by the Plan's Privacy Officer.

5. Definition of Limited Data Set. A limited data set is PHI that excludes the following direct identifiers of the individual to whom the PHI pertains or of relatives, employers, or household members of the individual:
  - (a) names;
  - (b) postal address information, other than town or city, State, and zip code;
  - (c) telephone numbers;
  - (d) fax numbers;
  - (e) electronic mail addresses;
  - (f) social security numbers;
  - (g) medical record numbers;
  - (h) Health Plan beneficiary numbers;
  - (i) account numbers;
  - (j) certificate/license numbers;
  - (k) vehicle identifiers and serial numbers, including license plate numbers;
  - (l) device identifiers and serial numbers;
  - (m) web Universal Resource Locators (URLs);
  - (n) internet Protocol (IP) address numbers;
  - (o) biometric identifiers, including finger and voice prints; and
  - (p) full face photographic images and any comparable images.
  
6. Violations of Agreement. If any representative of the Plan knows of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the data use agreement, that person shall report the activity or practice to the Privacy Officer who shall ensure that reasonable steps are taken to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful:
  - (a) disclosures of PHI to the recipient are discontinued; and
  - (b) the problem is reported to the Secretary of the Department of Health and Human Services.
  
7. Reporting Violations. Determinations of whether disclosures will be discontinued or problems will be reported to the Secretary of the Department of Health and Human Services shall be made by the Plan's Privacy Officer.

## **POLICY AND PROCEDURE FOR MINIMUM NECESSARY REQUIREMENT**

### **Purpose**

The Privacy Regulations establish the Plan's obligation to use, disclose or request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request.

### **Policy**

1. When using or disclosing PHI, or when requesting PHI from another Covered Entity (Health Care Provider, Health Plan, or Health Care Clearinghouse), the Plan will 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," the Plan 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. For an explanation of the limited data set, see the Policy and Procedure for Limited Data Set (page 16).
2. Exceptions to the minimum necessary requirement include:
  - (a) uses or disclosures made to the individual who is the subject of the information;
  - (b) uses or disclosures made pursuant to an authorization;
  - (c) disclosures made to the Secretary of the Department of Health and Human Services pursuant to a privacy investigation;
  - (d) uses and disclosures that are Required By Law; and
  - (e) uses or disclosures that are required by the Privacy Regulations or other laws.
3. Employees who perform services on behalf of the Plan will be trained to apply the "minimum necessary" principle to the use and disclosure of PHI. The Privacy Officer will also ensure that Business Associates are contractually required to abide by this Policy. TPA is a Business Associate and may access, use, disclose, and request PHI only as necessary to perform the services referred to in its Business Associate agreement with the Plan, which includes, but is not limited to, record-keeping and other administrative activities. TPA is expected to follow the "minimum necessary" principle when sharing PHI with any subcontractors whom it engages to perform administrative activities.

### **Procedure**

1. Identification of Persons Who Need Access. The Plan has identified the following persons in the Plan Sponsor's Workforce who need access to PHI to carry out their duties (position titles are subject to change by the Plan Sponsor, and any position entitled to access to PHI under this Policy shall refer to the title of such position then in effect):
  - (a) Privacy Officer may access PHI necessary to enforce the Plan's privacy policies and procedures or as necessary to perform any plan administrative functions, including, but not limited to, adjudicating appeals for claims denials and addressing claims questions.
  - (b) Service Center Staff, BES, BPA, BPC and RM may view Plan Sponsor and participant demographic information and transactions (e.g., disbursements from the Plan to reimburse plan participants) to monitor Plan eligibility and enrollment, reconcile Plan payments, and respond to participant inquiries.
  - (c) MERS Hearing Officers: Any PHI necessary for claims resolution between participants and the Plan, including, but not limited to, adjudicating appeals for claims denials and addressing claims questions.

- (d) Senior Management: Only aggregated non-identifiable information, unless minimally necessary to perform a Plan administrative function such as determining final appeals of claims.
  - (e) Others: In his or her discretion, the Privacy Officer may, from time to time, designate other individuals or classes of individuals to use PHI. The Privacy Officer shall identify such individuals and define the PHI they may use. Individuals performing services on behalf of the Plan will not access the PHI of any participant or dependent that is not relevant to the particular job they are performing for the Plan. All such individuals shall be trained in the use and disclosure of PHI consistent with the Policy and Procedure for Employee Education and Discipline (page 46).
2. Requests to Others. When requesting information from other entities, such as Health Plans or medical providers, the Plan will limit its own requests for PHI to the minimum necessary to accomplish the purpose for which the request is made.
  3. Routine and Recurring Requests to Others. If the Plan identifies routine and recurring requests that it makes of others for PHI, the Plan will implement policies and procedures (which may be standard protocols) that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.
  4. Entire Record. The Plan may not use, disclose or request an entire billing record, except when the entire record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.
  5. Reliance. When making minimum necessary determinations, the Privacy Officer may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when;
    - (a) Making disclosures to public officials that are permitted under the Privacy Regulations, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);
    - (b) The information is requested by another Covered Entity;
    - (c) The information is requested by a professional who is a member of the Plan's Workforce or is a Business Associate of the Plan for the purpose of providing professional services to the Plan, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or
    - (d) Documentation or representations that comply with the applicable requirements of the Privacy Regulations have been provided by a person requesting the information for research purposes.
  6. De-Identified Information. Whenever possible, the Plan should use and disclose only de-identified information (see Policy and Procedure for De-Identification, page 23), unless the identity of an individual is a part of the minimally necessary amount of information needed to accomplish the purpose of the use or disclosure.

# **POLICY AND PROCEDURE FOR VERIFICATION OF INDIVIDUAL'S IDENTITY AND AUTHORITY**

## **Purpose**

The Plan may disclose PHI only to those individuals who have a legal right to receive the PHI. This Policy describes the Plan's procedures for verifying an individual's identity and authority before disclosing PHI to that individual.

## **Policy**

Prior to any disclosure of PHI, the Plan must verify the authority and identity of the individual to whom the disclosure is to be made. The verification requirements are met if the Plan exercises professional judgment in using or disclosing PHI in accordance with the Policy and Procedure on Agreements (page 6) or acts on a good faith belief in disclosing PHI to avert a serious threat to health or safety.

## **Procedure**

1. **Request.** Prior to making any disclosure of PHI to an individual, the Plan will verify the individual's identity (if the person acting on behalf of the Plan does not otherwise know the individual) by requesting the following:
  - (a) The name and address of the person seeking the disclosure and his or her relationship to the individual whose PHI is being sought; and
  - (b) The name, address, and social security number of the person whose PHI is being sought.
2. **Documents.** When a disclosure is conditioned on particular documentation, statements, or representations from the person making the request, the Plan may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements. For example, when applicable, the Plan should request a power of attorney, letter of guardianship, or evidence of other legal authority to act on behalf of another individual and may rely upon such documentation.
3. **Reliance Regarding Identity of Public Officials.** The Plan may rely, if such reliance is reasonable under the circumstances, on any of the following to verify the identity of an individual when the disclosure of PHI is to a public official or a person acting on behalf of the public official:
  - (a) if the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
  - (b) if the request is in writing, the request is on the appropriate government letterhead; or
  - (c) if the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority 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.
4. **Reliance Regarding Authority of Public Officials.** The Plan may rely, if such reliance is reasonable under the circumstances, on any of the following to verify the authority of an individual when the disclosure of PHI is to a public official or a person acting on behalf of the public official:
  - (a) 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;

- (b) if a 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 is presumed to constitute legal authority.

## **POLICY AND PROCEDURE FOR DE-IDENTIFICATION**

### **Purpose**

The Privacy Regulations allow the Plan to de-identify PHI in order to use and disclose such information without being subject to the limitations set forth by the Privacy Regulations.

### **Policy**

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, is not Individually Identifiable Health Information. Such information is de-identified information and may be used without limitation. The information will only be used if the Plan does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

### **Procedure**

1. Method for Creating De-Identified Information. The Plan may determine that Health Information is not Individually Identifiable Health Information only if a person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
  - (a) applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
  - (b) documents the methods and results of the analysis that justify such determination.
  
2. Alternative Method for Creating De-Identified Information. In the alternative, de-identified information may be created by removing the following identifiers of the individual, or of relatives, employers, or household members of the individual:
  - (a) names;
  - (b) 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:
    - (i) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    - (ii) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
  - (c) 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;
  - (d) telephone numbers;
  - (e) fax numbers;
  - (f) electronic mail addresses;
  - (g) social security numbers;
  - (h) medical record numbers;
  - (i) Health Plan beneficiary numbers;
  - (j) account numbers;

- (k) certificate/license numbers;
  - (l) vehicle identifiers and serial numbers, including license plate numbers;
  - (m) device identifiers and serial numbers;
  - (n) web Universal Resource Locators (URLs);
  - (o) internet Protocol (IP) address numbers;
  - (p) biometric identifiers, including finger and voice prints;
  - (q) full face photographic images and any comparable images; and
  - (r) any other unique identifying number, characteristic, or code, except as permitted for purposes of re-identification.
3. Re-Identifying Information. The Plan may assign a code or other means of record identification to allow information that has been de-identified to be re-identified by the Plan, provided that:
- (a) the code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
  - (b) the Plan does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.
4. Providing De-Identified Information in Company Reports. From time to time, the Plan may need to disclose de-identified or aggregate information to appropriate Plan Sponsor personnel for legitimate business purposes such as analyses in financial reports and business planning. In all such cases, only de-identified information shall be used and individuals who receive such information shall be trained to maintain the confidentiality of such information and refrain from attempting to identify any individual to whom such de-identified information pertains. In cases where disclosure of such de-identified information is appropriate and authorized by this Policy and Procedure, only the minimum necessary amount of de-identified information should be provided and any breach of this Policy and Procedure should immediately be reported to the Privacy Officer and appropriate disciplinary action shall be taken. Individuals who receive any de-identified information that is authorized to be released under this Policy and Procedure shall not receive any bonuses, compensation, or other remuneration based on the information, nor on any factors related to the amount of costs incurred by the Plan for claims for health care expenses made under the Plan.
5. Privacy Officer Role. No PHI shall be converted into de-identified information and no de-identified information shall be used or disclosed by the Plan (including, but not limited to, the Plan's Business Associates) without the prior approval of the Privacy Officer.

## **POLICY AND PROCEDURE FOR NOTICE OF PRIVACY PRACTICES, COMPLAINTS, AND PRIVACY OFFICER**

### **Purpose**

The Privacy Regulations 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 the PHI. They also require the Plan to provide a means for individuals to lodge complaints about the Plan's uses and disclosures of their PHI. They also require the Plan to appoint a Privacy Officer to serve as the individual charged with leading and managing the implementation of privacy Policies and Procedures.

### **Policy**

The Plan will provide notice to all its participants of the ways that the Plan will use and disclose their PHI and their individual rights as required by the Privacy Regulations and will provide a means for individuals to lodge complaints about the uses and disclosures of their PHI. It will also appoint a Privacy Officer who shall have the responsibility of managing and implementing privacy Policies and Procedures.

### **Procedure**

1. **Timing and Content of Notice.** The Privacy Officer will provide the Plan's Notice of Privacy Practices ("Notice"):
  - (a) at the time of enrollment, to individuals who are new enrollees; and
  - (b) within 60 days of a material revision to the Notice, to individuals then covered by the Plan.

The Privacy Officer shall ensure that the Notice contains all of the elements required by the Privacy Regulations. For this purpose, the Privacy Officer may use a model notice issued by the U.S. Department of Health and Human Services.

2. **New Enrollees.** New enrollees will receive the Notice in their initial enrollment package, along with their summary plan description booklet and other initial notices.
3. **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. If there is a material change to the Notice:
  - (a) if the Plan posts its Notice on its web site, it must prominently post the change or its revised Notice on its web site by the effective date of the material change to the Notice, and provide the revised Notice, or information about the material change and how to obtain the revised Notice, in its next annual mailing to individuals then covered by the Plan.
  - (b) if the Plan does not post its Notice on a web site, it must provide the revised Notice, or information about the material change and how to obtain the revised Notice, to individuals then covered by the Plan within 60 days of the material revision to the Notice.
4. **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.

5. 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.
6. Web-Site. If The Plan 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.
7. Documentation. The Privacy Officer will document compliance with the notice requirements, by retaining copies of the Notice issued by the Plan for six years from the date of the Notice's creation or the date when it was last in effect, whichever is later.
8. Business Associates. The Privacy Officer shall ensure that each Business Associate of the Plan (including, without limitation, the TPA) 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.
9. Complaints. Any individual who believes that his or her privacy rights have been violated may lodge a complaint with the Plan by completing **Form 6 (Complaint Form for Violation of Privacy Rights)** and submitting it the Plan's Privacy Officer 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 the Department of Health and Human Services. The Privacy Officer 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 six years after the complaint is fully resolved. Neither the Plan, nor the Plan Sponsor, shall retaliate against any individual who lodges a complaint under this Policy and Procedure.
10. Privacy Officer. The Privacy Officer shall be appointed by the Plan Sponsor in its role as administrator of the Plan. The Privacy Officer will coordinate the development and implementation of the Plan's privacy Policies and Procedures. The Privacy Officer will have primary responsibility to manage, regularly monitor, and maintain compliance with the Plan's privacy Policies and Procedures and the requirements of the HIPAA Privacy Regulations. The Privacy Officer shall have all duties set forth in these Policies and Procedures and shall serve at the pleasure of the Plan Sponsor. The Privacy Officer's duties shall include those duties set forth elsewhere in these Policies and Procedures which include, without limitation:
  - (a) Assisting in development and implementation of policies and procedures to safeguard PHI, in coordination with the Security Officer.
  - (b) Ensuring that Plan Sponsor's employees receive regular privacy awareness updates and training.
  - (c) Creating an effective privacy Breach incident response policy and related procedures.
  - (d) Developing and implementing any corrective actions and notifications needed in response to privacy Breach incidents.
  - (e) Supervising the conduct of all employees in relation to the protection of PHI.
  - (f) Maintaining an inventory of all systems that contain Plan PHI.
  - (g) Conducting periodic risk analysis and audits of the Plan's privacy procedures in connection with the safeguarding of PHI.

- (h) Establishing procedures to initiate Business Associate agreements and drafting of agreement terms in order to effect compliance with the HIPAA Privacy and Security Regulations.
- (i) Overseeing the ongoing compliance of all Business Associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- (j) Serving as the designated Plan liaison to regulatory and accrediting bodies and trade associations, for matters relating to privacy and security.
- (k) Coordinating any response to complaints or compliance reviews for governmental or accrediting organizations concerning the Plan's compliance with state or federal privacy laws or regulations.
- (l) Overseeing individual rights to inspect, amend, and restrict access to PHI when appropriate.
- (m) Maintaining current knowledge of applicable federal and state privacy and security laws based on bulletins, updates, and other guidance.
- (n) Evaluating the selection, implementation, and administration of Plan privacy and security controls, including new privacy and security technologies as they become available.
- (o) Documenting, in writing, the actions taken in compliance with the Privacy Regulations, such as establishment of privacy compliant/incident logs.

## **POLICY AND PROCEDURE FOR AN INDIVIDUAL'S RIGHT TO REQUEST RESTRICTIONS**

### **Purpose**

The Privacy Regulations provide individuals with the right to request restrictions as to the use and disclosure of their PHI for purposes of Treatment, Payment, Health Care Operations, or to individuals involved in one's care or Payment for care. The Plan is not Required By Law to agree with such requests. However, if the Plan does agree, the PHI will be restricted as to use and disclosure, unless an emergency situation requiring such information's use or disclosure arises.

### **Policy**

1. The Plan will permit an individual to request that the Plan restrict the uses and/or disclosures of an individual's PHI in the following ways:
  - (a) to carry out Payment activities, or Health Care Operations, or
  - (b) to an individual's family members, other relatives, or close personal friends who may be involved in the individual's Payment for care.
2. The Plan is not required to agree to a request for restrictions, except as provided below.
3. If the Plan agrees to the request for a restriction, the Plan may still use or disclose the restricted PHI if needed for the individual's emergency.

### **Procedure**

1. To Request Restrictions. Any request for a restriction pursuant to this Policy must be submitted to the Plan's Privacy Officer in writing on **Form 2 (Request for Restrictions)**. Individuals may obtain the form by contacting the Privacy Officer (or on any form supplied by the Plan's TPA that complies with the Privacy Regulations).
2. If Restrictions Are Granted. If the Plan agrees to a restriction, the Privacy Officer will:
  - (a) document the agreed upon restriction and retain that documentation for a period of six years from the date of its creation or the date when it last was in effect, whichever is later; and
  - (b) notify the Plan's Workforce and TPA as to the restriction.
3. Required Restriction. The Plan must agree to the request of an individual to restrict disclosure of PHI about the individual to another Health Plan if:
  - (a) the disclosure is for the purpose of Payment or Health Care Operations (and is not otherwise Required By Law); and
  - (b) the PHI pertains solely to a health care item or service for which the individual, or person other than the Health Plan on behalf of the individual, has paid the Plan in full. This situation is likely to happen rarely and would likely only arise in a coordination of benefits scenario where an individual does not want a claim to be submitted to a primary plan and pays for the claim out-of-pocket.
4. Continued Use. Even if the Plan has agreed to a restriction, the Plan may continue to use and disclose PHI as follows:

- (a) to the individual whose PHI is being restricted;
  - (b) as Required By Law;
  - (c) for the purposes described in the Plan's Policy and Procedure on Public Policy Uses and Disclosures (page 10); or
  - (d) to the Secretary of the Department of Health and Human Services to investigate or determine the Plan's compliance with the Privacy Regulations.
5. Terminating Restrictions. The Plan may terminate its agreement to a restriction, if:
- (a) the individual agrees to or requests the termination in writing;
  - (b) the individual orally agrees to the termination and the oral agreement is documented; or
  - (c) except for a restriction described in paragraph 3 above, 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.
6. Documentation. When the Plan agrees to a restriction, the Privacy Officer shall document and retain the restriction for a period of six years from the date of its creation, or the date when it was last in effect, whichever is later.
7. Records Held by Plan Service Providers. If the Plan's Privacy Officer receives any request for restrictions as to the use or disclosure of information that may be maintained by the Plan's service providers, such as TPA or TPA's subcontractor, the Privacy Officer will inform such service providers 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 service providers, the Privacy Officer shall consult with the affected service providers to ensure they can comply with the request, if granted. The Plan shall require its service providers to forward to the Privacy Officer any requests for restrictions that they receive directly from individuals for a decision by the Plan. The Privacy Officer, by contract or otherwise, may allow a service provider to independently respond to a request with regard to PHI maintained by such service provider on behalf of the Plan pursuant to a service provider's standard policies and procedures that are consistent with this Policy and Procedure and the Privacy Regulations.

## **POLICY AND PROCEDURE FOR AN INDIVIDUAL'S RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS**

### **Purpose**

The Privacy Regulations provide individuals with the right to request to receive confidential communications of PHI from the Plan by alternative means or at alternative locations.

### **Policy**

The Plan will permit individuals to request to receive communications of PHI from the Plan by alternative means or at alternative locations. The Plan, subject to the other terms of this Policy and Procedure, will accommodate such reasonable requests. The Plan may require the individual to state that the disclosure of all or part of that information could endanger the individual.

### **Procedure**

1. To Request Confidential Communications. All requests for confidential communications must be submitted in writing on **Form 3 (Request for Confidential Communications)** (or on any form supplied by the Plan's TPA that complies with the Privacy Regulations) to the Plan's Privacy Officer. Individuals may obtain the form by contacting the Privacy Officer.
2. Conditions. The Plan may condition the provision of a reasonable accommodation on information as to how payment will be handled and specification of an alternative address or other method of contact.
3. Statement of Harm. The Plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
4. Notification and Implementation. The Privacy Officer will notify the individual as to the acceptance of the alternative means of communication, and will determine all relevant persons that must be notified of the individual's request (such as the Plan's TPA) and forward the instructions accordingly. The Plan shall use the alternative means of communication until the individual submits a new request pursuant to this Policy.
5. Records Held by Plan Service Providers. If the Plan's Privacy Officer receives any request for confidential communications as to information that may be maintained by Plan service providers, such as TPA or TPA's subcontractor, the Privacy Officer will inform such service providers 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 service providers, the Privacy Officer shall consult with the affected service providers to ensure they can comply with the request, if granted. The Plan shall require its service providers to forward to the Privacy Officer any requests for confidential communications that they receive directly from individuals for a decision by the Plan. The Privacy Officer, by contract or otherwise, may allow a service provider to independently respond to a request with regard to PHI maintained by such service provider on behalf of the Plan pursuant to a service provider's standard policies and procedures that are consistent with this Policy and Procedure and the Privacy Regulations.

6. Documentation. If the Plan agrees to a confidential communication pursuant to this Policy, it shall maintain documentation of its agreement to grant the request for at least six years after the Plan's agreement to use confidential communications is no longer in effect.

## **POLICY AND PROCEDURE FOR AN INDIVIDUAL'S RIGHT TO REQUEST TO INSPECT AND OBTAIN A COPY OF PHI**

### **Purpose**

The Privacy Regulations provide individuals with the right of access to inspect and obtain a copy of their PHI.

### **Policy**

1. An individual has a right of access to inspect and obtain a copy of their own PHI maintained by the Plan in a Designated Record Set. This right does not apply to information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
2. The Plan may deny an individual access to his or her own PHI without providing the individual an opportunity for review of that decision if:
  - (a) the Privacy Regulations do not require the Plan to provide the individual with access to the information (see paragraph 1 above); or
  - (b) the information was obtained from someone, other than a Health Care Provider, under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

### **Procedure**

1. To Request Access. An individual may request access to inspect or copy his or her own PHI by submitting the request in writing on **Form 1 (Request to Inspect and Copy Health Information)** (or on any form supplied by the Plan's TPA that complies with the Privacy Regulations) to the Plan's TPA or the Privacy Officer. Individuals may obtain the form by contacting the Privacy Officer or the TPA.
2. Designated Record Set. The Plan will permit an individual to request access to inspect or to obtain a copy of the PHI about the individual that is maintained in a "Designated Record Set," which is defined as the individual's enrollment, Payment and claims adjudication materials maintained by the Plan, or any other group of records used by the Plan to make decisions about the individual.
3. Timing of Response. The Plan will act on an access request no later than 30 days after receipt of the request, unless the Plan is unable to take action on the request within 30 days and follows the procedures for extension of time in paragraph 5 below.
4. Records Held by Plan Service Providers. If the Plan's Privacy Officer receives any request for information that may be maintained by the Plan's service providers (such as the Plan's TPA or TPA's subcontractor), the Privacy Officer will forward that request to the appropriate third party for handling consistent with the Privacy Regulations. The Plan may require such service providers to respond directly to the individual making the request, or may require the service provider to forward the PHI to the Plan to coordinate a response. If the service provider responds to the individual with anything less than the PHI requested, the service provider shall promptly notify the Privacy Officer. The Privacy Officer, by contract or otherwise, may allow a service provider to independently respond to a request with regard to PHI maintained by such service provider on behalf of the Plan pursuant to a service provider's standard policies and procedures

that are consistent with this Policy and Procedure and the Privacy Regulations. Currently, the Plan's Business Associate agreement with TPA provides for the following:

- (a) If TPA (or its subcontractor) receives a request to access a Designated Record Set directly from an individual, it must provide the Plan with written notice of the request within 30 days after the TPA receives the request;
- (b) After receiving TPA's written notice of an individual's access request, the Plan will either approve or disapprove the request and provide TPA written notice of its decision;
- (c) After receiving the Plan's written notice of its decision to approve or disapprove the individual's access request, the TPA must respond to the request in a manner that complies with the Privacy Regulations. For example, TPA may provide the individual with access to the Designated Record Set in a reasonable time and manner that is consistent with the Privacy Regulations; and
- (d) The Plan shall have sole responsibility and authority to approve or deny an individual's access request, even when such request is received directly by TPA.

5. Extensions of Time. If the Plan is unable to take an action within the time required, the Plan may extend the time for such actions by no more than 30 days, provided that:

- (a) the Plan, within the initial time for responding, provides the individual with a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request; and
- (b) the Plan may have only one such extension of time for action on a request for access.

6. If Access Is Granted. If the Plan (either directly or through its TPA) grants the access request, in whole or in part:

- (a) the Plan will provide the access requested within a timely manner;
- (b) the Plan may provide the information only once in response to any one request, even if it appears in more than one Designated Record Set;
- (c) the Plan will provide the access in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in such other form as agreed to by the Plan and the individual;
- (d) if the information is maintained electronically, the Plan will provide the information in the form and format requested by the individual if the information is readily producible; or, if not the Plan must provide the information in a readable electronic form as agreed to by the individual and the Plan;
- (e) the Plan may provide the individual with a summary of the PHI requested in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided, if:
  - (i) the individual agrees in advance to such a summary or explanation; and
  - (ii) the individual agrees in advance to the fees imposed, if any, by the Plan for such summary or explanation;
- (f) the Plan will arrange with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mail the copy of the PHI at the individual's request;
- (g) the Plan may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access;
- (h) if the individual requests a copy of the PHI or agrees to a summary or explanation of such information, the Plan may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
  - (i) labor for copying, the PHI requested by the individual, whether in paper or electronic form;
  - (ii) supplies for creating the paper copy or media if the individual requests that the electronic copy be provided on portable media;;

- (iii) postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
- (iv) preparing an explanation or summary of the PHI, if agreed to by the individual.

If the Plan (or TPA or TPA's subcontractor) receives any request for electronic information to be forwarded to a designated third party, the Plan (or TPA or TPA's subcontractor) will provide information to the third party. The individual's request to forward information to a third party must be in writing, clearly designate the third party, and be signed by the individual.

7. If Access Is Denied. If the Plan (either directly or through its TPA) denies access, in whole or in part:
- (a) the Plan will, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI as to which the Plan has reason to deny access;
  - (b) the Plan will provide a timely, written denial to the individual, in plain language, containing:
    - (i) the basis for the denial;
    - (ii) if applicable, a statement of the individual's review rights, including a description of how the individual may exercise such review rights; and
    - (iii) a description of how the individual may complain to the Plan or to the Secretary of the Department of Health and Human Services, including the name, or title, and telephone number of the contact person or office responsible to receive complaints;
  - (c) if the Plan does not maintain the PHI that is the subject of the individual's request for access, and the Plan knows where the requested information is maintained, the Plan will inform the individual where to direct the request for access; and
  - (d) 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:
    - (i) the Plan will promptly refer a request for review to such designated reviewing official;
    - (ii) the designated reviewing official will determine, within a reasonable period of time, whether or not to deny the access requested; and
    - (iii) the Plan will promptly provide written notice to the individual of the determination of the designated reviewing official.
8. Documentation. The Plan will document and retain the documentation for six years from the date of its creation or the date when it last was in effect, whichever is later:
- (a) the Designated Record Sets that are subject to access by individuals; and
  - (b) the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

## POLICY AND PROCEDURE FOR AN INDIVIDUAL'S RIGHT TO REQUEST AN AMENDMENT TO PHI

### **Purpose**

The Privacy Regulations provide individuals with the right to request an amendment to their PHI. Individuals may request to amend their PHI for as long as the Plan maintains it within a Designated Record Set.

### **Policy**

1. An individual has the right to request an amendment to PHI or a record about the individual in a Designated Record Set for as long as the PHI is maintained in the Designated Record Set by the Plan.
2. The Plan may deny an individual's request for amendment if it determines that the PHI or record that is the subject of the request:
  - (a) was not created by the Plan, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
  - (b) is not part of the Designated Record Set;
  - (c) would not be available for inspection as permitted by the Privacy Regulations and the Plan's Policy and Procedure for an Individual's Right to Request to Inspect and Obtain a Copy of PHI (page 32); or
  - (d) is accurate and complete.

### **Procedure**

1. To Request An Amendment. All requests that the Plan amend the PHI maintained in the Designated Record Set must be submitted in writing on **Form 4 (Request for Amendment to Health Information)** (or on any form supplied by the Plan's TPA that complies with the Privacy Regulations) and submitted to the Plan's Privacy Officer. All requests must provide a reason to support a requested amendment. Individuals may obtain the form by contacting the Privacy Officer.
2. Amendment Permitted. If the Plan grants an individual's request to amend his or her PHI, the amendment may only be made with respect to PHI that is:
  - (a) created by the Plan (or was created by someone who is no longer available to act on the request amendment); and
  - (b) maintained in a "Designated Record Set," which is defined as the individual's enrollment, Payment and claims adjudication materials maintained by the Plan, or any other group of records used by the Plan to make decisions about the individual.
3. Amendment Denied. The Plan will deny an individual's request to amend if the PHI:
  - (a) was not created by the Plan, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
  - (b) is not part of the Designated Record Set;
  - (c) would not be available for inspection as permitted by the Privacy Regulations; or
  - (d) is accurate and complete.

4. Timing of Response. The Plan (through the Privacy Officer) will respond to any amendment request within 60 days if possible. Otherwise, the Plan may extend the time for such action by no more than 30 days, provided that:
  - (a) within the original 60 day time period, the Plan provides the individual with a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request; and
  - (b) the Plan may have only one such extension of time for action on a request for an amendment.
  
5. If the Request Is Granted:
  - (a) the Plan will make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the Designated Record Set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment;
  - (b) the Privacy Officer will timely inform the individual that the amendment is accepted and obtain the individual's identification of, and agreement to, have the Plan notify the relevant persons with which the amendment needs to be shared; and
  - (c) the Privacy Officer will make reasonable efforts to inform and provide the amendment within a reasonable time to:
    - (i) persons identified by the individual as having received PHI about the individual and needing the amendment; and
    - (ii) persons, including Business Associates, that the Plan knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.
  
6. If the Request is Denied:
  - (a) the Privacy Officer will provide the individual with a timely, written denial which will use plain language and contain:
    - (i) the basis for the denial;
    - (ii) the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
    - (iii) a statement that, if the individual does not submit a statement of disagreement, the individual may request that the Plan provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and
    - (iv) a description of how the individual may complain to the Plan or to the Secretary of the Department of Health and Human Services, including the name, or title, and telephone number of the contact person or office responsible to receive complaints.
  - (b) the Privacy Officer will permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The Plan may reasonably limit the length of a statement of disagreement;
  - (c) the Plan may prepare a written rebuttal to the individual's statement of disagreement. The Privacy Officer shall make any determination of whether such a rebuttal will be prepared. Whenever such a rebuttal is prepared, the Privacy Officer will provide a copy to the individual who submitted the statement of disagreement;
  - (d) the Privacy Officer will, as appropriate, identify the record or PHI in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the Plan's denial of the request, the individual's statement of disagreement, if any, and the Plan's rebuttal, if any, to the Designated Record Set; and

- (e) upon the Plan's denial of an amendment, future disclosures, require the following:
  - (i) if a statement of disagreement has been submitted by the individual, the Plan will include the material appended, or, at the election of the Plan, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates;
  - (ii) if the individual has not submitted a written statement of disagreement, the Plan will include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI, only if the individual has requested such action; and
  - (iii) when a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, the Plan may separately transmit the material to the recipient of the standard transaction.
- 7. Amendments By Others. If the Plan is informed by another Covered Entity of an amendment to an individual's PHI, the Plan will amend the PHI within the Plan's Designated Record Sets and the Privacy Officer will inform any of the Plan's service providers who maintain affected PHI in a Designated Record Set of the amendment and cause them to make the amendment.
- 8. Documentation. The Plan will document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.
- 9. Records Held by Plan Service Providers. If the Plan's Privacy Officer receives any request to amend an individual's information that may be maintained by Plan service providers (such as the Plan's TPA or TPA's subcontractor), the Privacy Officer will inform such service providers of the Plan's decision with respect to such request and shall cause the service provider to comply with such decision (including making the amendment to the PHI, including statements of disagreement and rebuttals, and making the appropriate disclosures of the amendment, disagreement, and rebuttal in the future). Prior to making such a decision with regard to records held by the Plan's service providers, the Privacy Officer shall consult with the affected service providers to ensure they can comply with the request, if granted. The Plan shall require its service providers to forward to the Privacy Officer any requests for amendments that they receive directly from individuals for a decision by the Plan. The Privacy Officer, by contract or otherwise, may allow a service provider to independently respond to a request with regard to PHI maintained by such service provider on behalf of the Plan pursuant to a service provider's standard policies and procedures that are consistent with this Policy and Procedure and the Privacy Regulations. Currently, the Plan's Business Associate agreement with TPA provides for the following:
  - (a) If TPA (or its subcontractor) receives a request to amend a Designated Record Set directly from an individual, it must provide the Plan with written notice of the request within 30 days after the TPA receives the request; After receiving TPA's written notice of an individual's amendment request, the Plan will either approve or disapprove the request and provide TPA written notice of its decision;
  - (b) After receiving the Plan's written notice of its decision to approve or disapprove the individual's amendment request, the TPA must respond to the request in a manner that complies with the Privacy Regulations. For example, TPA may amend the Designated Record Set in a reasonable time and manner that is consistent with the Privacy Regulations; and
  - (c) The Plan shall have sole responsibility and authority to approve or deny an individual's amendment request, even when such request is received directly by TPA.

## POLICY AND PROCEDURE FOR AN INDIVIDUAL'S RIGHT TO REQUEST AN ACCOUNTING OF DISCLOSURES

### **Purpose**

The Privacy Regulations provide individuals with the right to request an accounting of certain disclosures made by the Plan of an individual's PHI.

### **Policy**

1. An individual has a right to receive an accounting of certain disclosures of PHI made by the Plan in the six years prior to the date on which the accounting is requested, including, but not limited to:
  - (a) any disclosures not permitted by the Privacy Regulations or these Policies (including inadvertent or mistaken disclosure);
  - (b) any disclosures the Plan makes pursuant to a "public policy" purpose as set forth in these Policies (page 10);
  - (c) any disclosures Required By Law; and
  - (d) any disclosures made pursuant to an administrative or judicial order, subpoena, discovery request, QMCSO, or workers' compensation program.
  
2. The Plan need not provide an accounting of the following types of disclosures of PHI:
  - (a) to carry out Payment, and Health Care Operations;
  - (b) to individuals of PHI about themselves;
  - (c) incident to a use or disclosure otherwise permitted or required by the Privacy Regulations;
  - (d) pursuant to an authorization;
  - (e) for national security or intelligence purposes;
  - (f) to correctional institutions or Law Enforcement Officials related thereto; or
  - (g) as part of a limited data set.

### **Procedure**

1. To Request an Accounting. To request an accounting of disclosures of PHI, an individual must submit a request in writing to the Plan's Privacy Officer on **Form 5 (Request for an Accounting of Disclosures)** (or any form supplied by the Plan's TPA that complies with the Privacy Regulations). Individuals may obtain the form by contacting the Privacy Officer.
  
2. Logging Disclosures. In order to comply with this accounting obligation, the Plan's Privacy Officer will keep a log of the disclosures that are not identified in item 2 in the Policy Section above. Anyone who makes a disclosure on behalf of the Plan that is not listed in item 2 of the Policy Section above must immediately inform the Privacy Officer of such disclosure so that the Privacy Officer may log the disclosure. The Privacy Officer, through Business Associate contracts, shall cause the Plan's service providers (such as the Plan's TPA or TPA's subcontractor), to maintain such a log as well and to report accountable disclosures to the Privacy Officer or to an individual when requested. For example, through a Business Associate agreement, the Plan currently requires TPA to keep a log of the following information for each disclosure of PHI made by TPA: (i) the date of the disclosure; (ii) the name of the entity or person who received the PHI and, if known, the address of such entity or person; (iii) a brief description

of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably states the basis for the disclosure.

3. Information Provided in Accounting. The Plan's log and any written accounting provided by the Plan will include:
  - (a) those disclosures identified above that occurred during the six years (or such shorter time period at the request of the individual) prior to the date of the request for an accounting, including disclosures to or by Business Associates of the Plan; and
  - (b) for each disclosure:
    - (i) the date of the disclosure;
    - (ii) the name of the entity or person who received the PHI and, if known, the address of such entity or person;
    - (iii) a brief description of the PHI disclosed; and
    - (iv) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure that was permitted or Required By Law, if any.
  
4. Multiple Disclosures of Same Information. If, during the period covered by the accounting, the Plan has made multiple disclosures of PHI to the same person or entity for a single purpose related to disclosures to the Secretary of the Department of Health and Human Services or for public policy reasons recognized in the Privacy Regulations, the accounting may, with respect to such multiple disclosures, provide:
  - (a) the information for the first disclosure during the accounting period;
  - (b) the frequency, periodicity, or number of the disclosures made during the accounting period; and
  - (c) the date of the last such disclosure during the accounting period.
  
5. Timing of Response. The Plan will act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows:
  - (a) the Plan will provide the individual with the accounting requested; or
  - (b) if the Plan is unable to provide the accounting within the 60 day period, the Plan may extend the time to provide the accounting by no more than 30 days, provided that:
    - (i) the Plan, within the original 60 day period, provides the individual with a written statement of the reasons for the delay and the date by which the Plan will provide the accounting; and
    - (ii) the Plan may have only one such extension of time for action on a request for an accounting.
  
6. Charge. The Plan will provide the first accounting to an individual in any 12 month period without charge. The Plan may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the Plan informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.
  
7. Documentation. The Plan will document the following and retain the documentation for six years from the date of its creation or the date when it last was in effect, whichever is later:
  - (a) the written accounting that is provided to the individual requesting an accounting; and
  - (b) the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

8. Suspension of Accounting Right. The Plan will temporarily suspend an individual's right to receive an accounting of disclosures to a Health Oversight Agency or Law Enforcement Official for the time specified by such agency or official, if such agency or official provides the Plan with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required. If the agency or official statement is made orally, the Plan will:
  - (a) document the statement, including the identity of the agency or official making the statement;
  - (b) temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and
  - (c) limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.
  
9. Accounting of Disclosures by Plan Service Providers. If the Plan's Privacy Officer receives for an accounting of disclosures of an individual's information made by Plan service providers (such as the Plan's TPA or TPA's subcontractor), the Privacy Officer will forward that request to the appropriate third party and request the service provider (in the Privacy Officer's discretion) to provide the requested accounting either directly to the requesting individual or to the Privacy Officer who will organize a coordinated response from the Plan. The Privacy Officer, by contract or otherwise, may allow a service provider to independently respond to a request with regard to PHI maintained by such service provider on behalf of the Plan pursuant to a service provider's standard policies and procedures that are consistent with this Policy and Procedure and the Privacy Regulations. Currently, the Plan's Business Associate agreement with TPA provides for the following:
  - (a) If TPA (or its subcontractor) receives a request for an accounting of disclosures directly from an individual, it must provide the Plan with written notice of the request within 30 days after the TPA receives the request.
  - (b) After receiving TPA's written notice of an individual's request for an accounting, the Plan will determine whether it is acceptable for TPA to respond directly to the individual. TPA shall not provide an accounting of disclosures directly to the individual unless the Plan has directed it to do so.
  - (c) If the Plan directs TPA to directly respond to the individual's request for an accounting, then TPA must provide the individual with information sufficient to satisfy the Privacy Regulations' requirements for an accounting of disclosures.

## **POLICY AND PROCEDURE FOR SECURING PHI AND NOTIFICATION IN CASE OF BREACH OF UNSECURED PHI**

### **Purpose**

The HITECH Act requires the Plan to follow certain notification procedures in the event of a Breach of Unsecured PHI. The Secretary of the Department of Health and Human Services has issued guidance specifying the technologies and methodologies that render PHI secured. PHI that is not secured in accordance with the guidance is subject to the Breach notification rules described in this Policy.

### **Policy**

1. The Plan will endeavor to secure all PHI in accordance with the guidance issued by the Secretary of the Department of Health and Human Services. Secured PHI is not subject to the Breach notification rules described in this Policy.
2. The Plan will implement reasonable systems for discovery of Breaches of PHI, both internally and with its Business Associates, to ensure the timely compliance with all notice requirements in the event of a Breach of Unsecured PHI. The Privacy Officer will also ensure that Business Associates are contractually required to abide by this Policy.
3. The Plan will conduct a risk assessment and document its determination of whether or not a Breach of PHI has occurred.
4. In instances where it is impracticable to render PHI secure, or PHI is otherwise not secured, and there is a Breach of such Unsecured PHI, the Plan will follow the Breach notification procedures, as set forth below.

### **Procedure**

1. Endeavor to Secure All PHI. 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.
  - (a) *Encryption.* With respect to electronic PHI, the Plan will use one of the valid encryption processes for data at rest and for data in motion that is consistent with the published guidance from the National Institute of Standards and Technology.
  - (b) *Destruction.* With respect to paper, film, or other hard copy media on which the PHI is stored or recorded, the Plan will shred or destroy the media, such that the PHI cannot be read or reconstructed. The Plan will not use redaction as a means of data destruction. With respect to electronic media, the Plan will clear, purge, or destroy the media consistent with the published guidance from the National Institute of Standards and Technology, such that the PHI cannot be retrieved.
2. Determination of Breach and Risk Assessment. The Privacy Officer will identify PHI that was the subject to the unauthorized acquisition, access, use, or disclosure and determine whether it was secured (*e.g.*, encrypted or secured). If the PHI was secured, no Breach occurred.

If the PHI was not secured, determine whether the unauthorized acquisition, access, use, or disclosure falls into an exception to the definition of Breach. The Privacy Officer will determine:  
(a) whether the unauthorized acquisition, access, use, or disclosure was unintentional and done by

a Workforce member or person acting under the authority of the Plan; and (b) whether it made in good faith and within the scope of authority of the person who made it; and (c) whether the unauthorized acquisition, access, use, or disclosure not result in further use or disclosure in a manner not permitted under the Privacy Regulations. If yes, then no Breach occurred. If no, the analysis must continue.

The Privacy Officer will determine: (a) whether the unauthorized acquisition, access, use, or disclosure an inadvertent disclosure by a person who is authorized to access PHI by the Plan to another person authorized to access PHI at the Plan; and (b) whether the information received as a result of such disclosure was not further used or disclosed in a manner not permitted under the Privacy Regulations. If yes, no Breach occurred. If no, the analysis must continue.

The Privacy Officer will determine whether there is a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. If yes, no Breach occurred. If no, the risk assessment must be done.

An impermissible use or disclosure of PHI is presumed to be a Breach, and therefore, notification to the individual will be given by the Privacy Officer, unless the Plan demonstrates that there is a low probability that the PHI has not been compromised based upon a four-part risk assessment.

(a) *Risk Assessment.* The four-part risk assessment includes:

- (i) The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification. To assess this factor, consider the type of PHI involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature. For example, with respect to financial information, this includes credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. With respect to clinical information, this may involve considering not only the nature of the services or other information, but also the amount of detailed clinical information involved. Considering the type of PHI involved in the impermissible use or disclosure will help determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests. Additionally, in situations where there are few, if any, direct identifiers in the information impermissibly used or disclosed, determine whether there is a likelihood that the PHI released could be reidentified based on the context and the ability to link the information with other available information. For example, if a Plan impermissibly disclosed a list of patient names, addresses, and hospital identification numbers, the PHI is obviously identifiable, and a risk assessment likely would determine that there is more than a low probability that the information has been compromised, dependent on an assessment of the other factors discussed below. Alternatively, if the Plan disclosed a list of patient discharge dates and diagnoses, the any of the individuals could be identified based on the specificity of the diagnosis, the size of the community served by the Plan, or whether the unauthorized recipient of the information may have the ability to combine the information with other available information to re-identify the affected individuals (considering this factor in combination with the second factor discussed below).
- (ii) The unauthorized person who used the PHI or to whom the disclosure of PHI was made. The second factor requires the Privacy Officer to consider the

unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made. Consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information. For example, if PHI is impermissibly disclosed to another entity obligated to abide by the HIPAA Privacy and Security Rules or to a Federal agency obligated to comply with the Privacy Act of 1974 and the Federal Information Security Management Act of 2002, there may be a lower probability that the PHI has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the Plan. If the information impermissibly used or disclosed is not immediately identifiable, determine whether the unauthorized person who received the PHI has the ability to re-identify the information. For example, if information containing dates of health care service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may be more than a low probability that the PHI has been compromised.

- (iii) Whether the PHI was actually viewed or acquired or, alternatively, if only the opportunity existed for the information to be viewed or acquired. The third factor requires the Privacy Officer to investigate an impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed. For example, if a laptop computer was stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the Privacy Officer could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed. In contrast, however, if information was mailed to the wrong individual who opened the envelope and called the Plan to say that she received the information in error, then, in this case, the unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error.
- (iv) The extent to which the risk to the PHI has been mitigated. Consider the extent to which the risk to the PHI has been mitigated. Attempt to mitigate the risks to the PHI following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. Privacy Officer should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised. For example, a Plan may be able to obtain and rely on the assurances of an employee, affiliated entity, Business Associate, or another Covered Entity that the entity or person destroyed information it received in error, while such assurances from certain third parties may not be sufficient.

3. Implement Reasonable Systems for Discovery of Breaches of PHI. Because it may not be possible or practicable to secure all PHI through encryption and destruction, the Privacy Officer will be responsible for implementing reasonable systems for discovery of Breaches of PHI, both internally and with its Business Associates, to ensure the timely compliance with all notice requirements in the event of a Breach of Unsecured PHI.

- (a) *Workforce Members.* The Privacy Officer 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), in accordance with the Policy and Procedure for Employee Education and Discipline (page 42). Workforce members who believe there may have been a Breach of Unsecured PHI shall notify the Privacy Officer immediately.
- (b) *Amendment of Business Associate Contracts.* 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.
- (c) *Investigation of Potential Breaches.* The Privacy Officer 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.

4. Notification of Individuals.

- (a) *General Rule.* 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.
- (b) *Breaches Treated as Discovered.* 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.
- (c) *Timeliness.* 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.
- (d) *Content.* The notification provided to the individual will include the following information in plain language:
  - (i) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
  - (ii) 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);
  - (iii) Any steps individuals should take to protect themselves from potential harm resulting from the Breach;
  - (iv) 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
  - (v) 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.
- (e) *Methods of Notification.* 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 Plan 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.

5. 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.
6. Notification to the Secretary. The Plan will notify the Secretary of the Department of Health and Human Services 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 Plan 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 were discovered. The Plan will provide information about any Breaches to the Secretary in the manner specified on the Department of Health and Human Services website.
7. 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, but shall specify that the notification be made without unreasonable delay and in no case later than 60 days after discovery of the Breach. For example, the Plan's current Business Associate contract with TPA requires TPA to notify the Plan of a Breach of Unsecured PHI within forty-eight (48) hours of when the TPA discovers the incident.
8. Law Enforcement Delay. The Plan will delay the notification required under this Policy 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 Officer will document the request and the identity of the official making the statement.
9. Documentation of Impermissible Uses and Disclosures. In the case of any impermissible use or disclosure of PHI, the Privacy Officer shall maintain documentation to demonstrate that all required notifications were made under this Policy, or, alternatively, that a risk assessment was conducted and the Plan determined the impermissible use or disclosure did not constitute a Breach of Unsecured PHI, and therefore notifications were not required.

## **POLICY AND PROCEDURE FOR EMPLOYEE EDUCATION AND DISCIPLINE**

### **Purpose**

The Privacy Regulations require that all members of the Plan's Workforce be educated and trained as to the appropriate manner of handling PHI in order to carry out their job functions and that Workforce members who fail to comply with the Plan's privacy policies and procedure be appropriately sanctioned.

### **Policy**

The Plan will train all members of its Workforce on the importance of privacy and the Plan's policies and procedures with respect to PHI, as necessary and appropriate for the members of the Workforce to carry out their function within the Plan.

### **Procedure**

1. Identifying Workforce and Timing of Training. The Privacy Officer 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." The Privacy Officer will ensure that each member of the Plan's Workforce receives training according to the following schedule:
  - (a) to each new member of the Workforce within a reasonable period of time after the person joins the Plan's Workforce; and
  - (b) 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.

2. Content of Training. Training will involve an overview of the Plan's obligations under the 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.
3. Documentation of Training. The Plan's Privacy Officer will document the content, date, and attendance at each of the training sessions as described above and will retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.
4. Sanctions. Members of the Plan's Workforce who use or disclose an individual's PHI in violation of the training provided, the Privacy Regulations, or these Policies and Procedures will be subject to sanctions that will be consistent with the nature of the violation. Such sanctions may include, but not be limited to, verbal and written warnings, suspensions, and termination. Sanctions will be imposed by the Plan Sponsor in consultation with the Privacy Officer who will document any sanctions that are imposed.

## **Policy and Procedure For Administrative, Physical, And Technical Safeguards For PHI**

### **Purpose**

The Plan shall make reasonable efforts to implement and administer reasonable administrative, physical, and technical safeguards for PHI.

### **Policy**

It is the policy of the Plan to address compliance with the HIPAA Privacy Regulations by having in place appropriate administrative, technical and physical safeguards to protect the privacy of Protected Health Information from an intentional or unintentional use or disclosure that is in violation of the Privacy and/or Security Regulations. It is also the policy of the Plan to have in place reasonable safeguards to limit incidental uses or disclosures made as part of an otherwise permitted or required use or disclosure. The PHI that is to be safeguarded may be in the form of oral, electronic, or paper communications.

### **Procedure**

1. Administrative Safeguards. Administrative safeguards that the Plan will implement and observe include but are not limited to the following:
  - (a) Oral Communications.
    - (i) Employees must take care to avoid unnecessary disclosures of PHI through oral communications. Voices must be modulated and attention paid to authorized listeners to avoid unnecessary disclosures.
    - (ii) PHI should be disclosed during oral conversations only when necessary for Payment or Health Care Operations purposes.
    - (iii) Telephone conversations should be conducted away from public areas if possible, such as hallways, bathrooms, cafeteria, kitchen, etc.
    - (iv) Speakerphones should be used only in private areas.
  - (b) Fax Communications
    - (i) Only the minimum necessary PHI to meet the requesting party's needs may be faxed.
    - (ii) Employees must regularly check and monitor their own fax and print jobs.
    - (iii) For unfamiliar or non-routine faxes, the employee must call to confirm receipt.
    - (iv) Employees must program the fax machine auto-dial with frequently used numbers to reduce errors in dialing.
    - (v) Employees must call ahead and verify non-routine numbers.
    - (vi) Employees must double-check the number that has been dialed into the fax machine, before sending the fax.
    - (vii) Employees are to auto-print transmission reports to document where the fax was sent.
    - (viii) The fax machine header must be set with the correct date, time, and name of facility or office.
    - (ix) "In-boxes" adjacent to the fax machine are to be set up, and responsibility designated to check and distribute documents regularly, so that faxes containing Health Information are not left lying around.
    - (x) Unclaimed items must be shredded regularly after a set time period after confirming materials are not needed.

- (xi) If a fax containing Health Information is received in error, then the sender must be notified to inform the sender of the mistake. The date, time, name of entity, and phone number must be logged, and then shred the fax.
  - (xii) If a fax is sent in error: the sender must notify the Privacy Officer.
  - (xiii) Fax machines are to be located in secure areas not readily accessible to visitors or patients.
  - (xiv) The applicable Plan Sponsor fax cover sheet must be used with each fax transmission, which includes information on the source of the fax (e.g., facility name, address, phone number, fax number) and an appropriate confidentiality notice.
- (c) Mail Communications
- (i) Any PHI that is mailed must be in a sealed envelope.
  - (ii) Any PHI mailed must be sent via first class or express mail.
- (d) Destruction Standards
- (i) Materials containing PHI must be discarded in a manner that maintains the confidentiality of such information.
  - (ii) Printed materials (such as faxes, copies of patient notes, etc.) that contain PHI may not be placed in trash bins, unsecured recycle bins, or other publicly accessible locations.
  - (iii) Printed materials must be personally shredded in a crosscut shredder or placed in secured shredder bins.
  - (iv) Electronic media must be destroyed.
2. Technical Safeguards. The Plan will implement and observe technical safeguards through the adoption and use of security policies and procedures and shall apply such security policies and procedures to ePHI maintained by the Plan, as applicable.
3. Physical Safeguards. Physical safeguards that the Plan will implement and observe include but are not limited to the following:
- (a) Paper records containing PHI must be stored or filed in such a way as to avoid access by unauthorized persons.
  - (b) Paper records containing PHI on desks or other work areas must be placed face down or concealed to avoid access by unauthorized person.
  - (c) Paper records containing PHI must be secured when a work area is unattended.
  - (d) Individuals who are not a part of the Plan's Workforce must be appropriately escorted and monitored when in areas containing Plan PHI.
  - (e) Any theft or loss of records must be reported immediately to the Privacy Officer so that mitigation measures may be reviewed and implemented.
  - (f) All papers containing PHI to be discarded must be placed in the shred bin, which is to be emptied on an as needed basis.
  - (g) Desktops must be cleared of materials containing PHI at the end of the business day. All drawers and cabinets are to be locked. All material containing PHI must be placed in locked files or locked desk drawers.
  - (h) Storage rooms containing PHI materials are to be locked when authorized employees are not present.
  - (i) Computer Workstations
    - (i) Workstations at the facility must have the monitor positioned away from common areas, or a privacy screen must be installed to prevent unauthorized access or view.
    - (ii) Employees must log off when done working on a computer workstation. The computer session must be locked when it is left unattended.

4. Privacy Officer Review. The Privacy Officer will assess and update the safeguards in place periodically.

## GLOSSARY

### **Breach**

1. The acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the Privacy Regulations which compromises the security or privacy of the Protected Health Information.
2. *Breach* excludes:
  - (a) Any unintentional acquisition, access, or use of Protected Health Information by a Workforce member or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Regulations.
  - (b) Any inadvertent disclosure by a person who is authorized to access Protected Health Information at a Covered Entity or Business Associate to another person authorized to access Protected Health Information at the same Covered Entity or Business Associate, 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.
  - (c) A disclosure of Protected Health Information where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
3. An acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the Privacy Regulations is presumed to be a Breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the following factors:
  - (a) The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification;
  - (b) The unauthorized person who used the Protected Health Information or to whom the disclosure was made;
  - (c) Whether the Protected Health Information was actually acquired or viewed; and
  - (d) The extent to which the risk to the Protected Health Information has been mitigated.

### **Business Associate**

1. Except as provided in paragraph (4) of this definition, *Business Associate* means, with respect to a Covered Entity, a person who:
  - (a) On behalf of such Covered Entity, but other than in the capacity of a member of the Workforce of such Covered Entity or arrangement, creates, receives, maintains, or transmits Protected Health Information for a function or activity regulated by the Privacy Regulations, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, Patient Safety Activities, billing, benefit management, practice management, and repricing; or
  - (b) Provides, other than in the capacity of a member of the Workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, where the provision of the service involves the disclosure of Protected Health Information from

such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

2. A Covered Entity may be a Business Associate of another Covered Entity.
3. Business Associate includes:
  - (a) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to Protected Health Information to a Covered Entity and that requires access on a routine basis to such Protected Health Information.
  - (b) A person that offers a personal health record to one or more individuals on behalf of a Covered Entity.
  - (c) A subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of the Business Associate.
4. Business Associate does not include:
  - (a) A Health Care Provider, with respect to disclosures by a Covered Entity to the Health Care Provider.
  - (b) A plan sponsor, with respect to disclosures by a Group Health Plan (or by a Health Insurance Issuer or HMO with respect to a Group Health Plan) to the plan sponsor.
  - (c) A government agency, with respect to determining eligibility for, or enrollment in, a government Health Plan that provides public benefits and is administered by another government agency, or collecting Protected Health Information for such purposes, to the extent such activities are authorized by law.

#### **Covered Entity**

1. A Health Plan.
2. A Health Care Clearinghouse.
3. A Health Care Provider who transmits any Health Information in electronic form in connection with a transaction covered by this subchapter.

#### **Data Aggregation**

With respect to PHI created or received by a Business Associate in its capacity as the Business Associate of a Covered Entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the Health Care Operations of the respective covered entities.

#### **Designated Record Set**

1. A group of records maintained by or for a Covered Entity that is:
  - (a) The billing records about individuals maintained by or for a covered Health Care Provider;
  - (b) The enrollment, Payment and claims adjudication record systems maintained by or for a Health Plan; or
  - (c) Used, in whole or in part, by or for the Covered Entity to make decisions about individuals.

2. For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity.

### **Disclosure**

The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

### **Financial Remuneration**

The direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any Payment for Treatment of an individual.

### **Group Health Plan (also see definition of Health Plan)**

A plan sponsored by the Plan Sponsor that is an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg– 91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

1. Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
2. Is administered by an entity other than the Plan Sponsor.

### **HHS**

The United States Department of Health and Human Services.

### **Health Care**

Care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

### **Health Care Clearinghouse**

A public or private entity, including a billing service, repricing company, community health management information system or community Health Information system, and "value-added" networks and switches, that does either of the following functions:

1. Processes or facilitates the processing of Health Information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

2. Receives a standard transaction from another entity and processes or facilitates the processing of Health Information into nonstandard format or nonstandard data content for the receiving entity.

### **Health Care Operations**

Any of the following activities of a Covered Entity to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities;
2. Conducting or arranging for legal services, and auditing functions, including fraud and abuse detection and compliance programs;
3. 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
4. Business management and general administrative activities of the entity, including, but not limited to:
  - (a) Management activities relating to implementation of and compliance with the requirements of this subchapter;
  - (b) 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;
  - (c) Resolution of internal grievances;
  - (d) 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
  - (e) Creating de-identified Health Information or a limited data set, and fundraising for the benefit of the Covered Entity.

### **Health Care Provider**

A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

### **Health Information**

Any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a Health Care Provider, Health Plan, Public Health Authority, employer, life insurer, school or university, or Health Care Clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

### **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

The federal law that resulted in the promulgation of the Privacy Regulation, governing the use and disclosure of protected health information held by covered entities, which this Policy seeks to comply.

**Health Insurance Issuer (as defined in section 2791(b)(2) of the Public Health Service Act, 42 U.S.C. 300gg–91(b)(2) and used in the definition of *Health Plan* in this section)**

An insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a Group Health Plan.

***Health Maintenance Organization (HMO)* (as defined in section 2791(b)(3) of the Public Health Service Act, 42 U.S.C. 300gg–91(b)(3) and used in the definition of *Health Plan* in this section)**

A federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

**Health Oversight Agency**

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.

**Health Plan**

An individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg–91(a)(2)).

1. *Health Plan* includes the following, singly or in combination:
  - (a) A Group Health Plan, as defined in this section.
  - (b) A Health Insurance Issuer, as defined in this section.
  - (c) An HMO, as defined in this section.
  - (d) Part A or Part B of the Medicare program under title XVIII of the Act.
  - (e) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, *et seq.*
  - (f) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).
  - (g) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
  - (h) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
  - (i) The health care program for active military personnel under title 10 of the United States Code.
  - (j) The veterans' health care program under 38 U.S.C. chapter 17.
  - (k) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).
  - (l) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*

- (m) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, *et seq.*
- (n) An approved State child Health Plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, *et seq.*
- (o) The Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28.
- (p) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
- (q) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

2. *Health Plan* excludes:

- (a) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg–91(c)(1); and
- (b) A government-funded program (other than one listed in paragraph (1)(i)–(xvi) of this definition):
  - (i) Whose principal purpose is other than providing, or paying the cost of, health care; or
  - (ii) Whose principal activity is: (A) the direct provision of health care to persons; or (B) the making of grants to fund the direct provision of health care to persons.

**HITECH Act**

The Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, as amended.

**Individual**

The person who is the subject of PHI.

**Individually Identifiable Health Information**

Information that is a subset of Health Information, including demographic information collected from an individual, and:

1. Is created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - (a) That identifies the individual; or
  - (b) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**LAN**

An acronym for Local Area Network.

## **Law Enforcement Officer**

An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an Officer inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

## **Marketing**

1. Except as provided in paragraph (2) of this definition, Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
2. Marketing does *not* include a communication made:
  - (a) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any Financial Remuneration received by the Plan in exchange for making the communication is reasonably related to the Plan's cost of making the communication.
  - 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, 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, except where the Plan receives Financial Remuneration in exchange for making the communication.

## **Patient Safety Activities**

The following activities carried out by or on behalf of a Patient Safety Organization or a provider:

1. Efforts to improve patient safety and the quality of health care delivery;
2. The collection and analysis of patient safety work product;
3. The development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices;
4. The utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk;
5. The maintenance of procedures to preserve confidentiality with respect to patient safety work product;
6. The provision of appropriate security measures with respect to patient safety work product;
7. The utilization of qualified staff; and

8. Activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system.

### **Patient Safety Organization**

A private or public entity or component thereof that is listed as a patient safety organization ("PSO") by the Secretary pursuant to 42 C.F.R. Part 3. A Health Insurance Issuer or a component organization of a Health Insurance Issuer may not be a PSO. See also the exclusions in § 3.102 of this part.

### **Payment**

1. The activities undertaken by:
  - (a) A Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Health Plan; or
  - (b) A Health Care Provider or Health Plan to obtain or provide reimbursement for the provision of health care; and
2. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:
  - (a) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication claims;
  - (b) Billing, claims management, collection activities, and related health care data processing;
  - (c) Review of health care services;
  - (d) Utilization review activities; and
  - (e) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of reimbursement:
    - (i) Name and address;
    - (ii) Date of birth;
    - (iii) Social security number;
    - (iv) Payment history;
    - (v) Account number; and
    - (vi) Name and address of the Health Care Provider and/or Health Plan.

### **Plan**

The Health Care Savings Program and any other Health Plans or programs of the Plan Sponsor providing medical care benefits (including health, dental, vision, long term care, or other coverage affecting any structure of the body) that are sponsored by the Plan Sponsor and that are subject to the Privacy Regulations and are either: (i) uninsured, or (ii) insured and provide PHI to the Plan Sponsor.

### **Plan Sponsor**

The participating employer, except that, for purposes of Code Section 4376, "Plan Sponsor" means the Board or, as appropriate in context, the Board through its agents.

### **Privacy Regulations**

The Standards for the Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.500 *et seq.*, as amended.

## **Protected Health Information or PHI**

Individually identifiable health or Genetic Information:

1. Except as provided in paragraph (2) of this definition, that is:
  - (a) Transmitted by electronic media;
  - (b) Maintained in any medium described in the definition of *electronic media*; or
  - (c) Transmitted or maintained in any other form or medium.
2. *PHI* excludes Individually Identifiable Health Information in:
  - (a) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g;
  - (b) Records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice as described at 20 U.S.C. 1232g(a)(4)(B)(iv);
  - (c) Employment records held by a Covered Entity in its role as employer; and
  - (d) Information about an individual who has been deceased for 50 years.

## **Public Health Authority**

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 Officer mandate.

## **Required By Law**

A mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law. *Required By Law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to Health Care Providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

## **Secretary**

The Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

## **State**

One of the following:

1. For a Health Plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such Health Plan.
2. For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

**Subcontractor**

A person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the Business Associate's Workforce.

**TPA**

The person or entity chosen by the Plan or the Plan Sponsor to assist the Plan with identified administrative functions such as claims administration or adjudication. The TPA is a Business Associate of the Plan.

**Treatment**

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.

**Unsecured Protected Health Information or Unsecured PHI**

Protected Health Information 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.

**Use**

With respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

**Workforce**

Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity.