TEACHER RETIREMENT SYSTEM OF TEXAS

HIPAA PRIVACY POLICIES & PROCEDURES

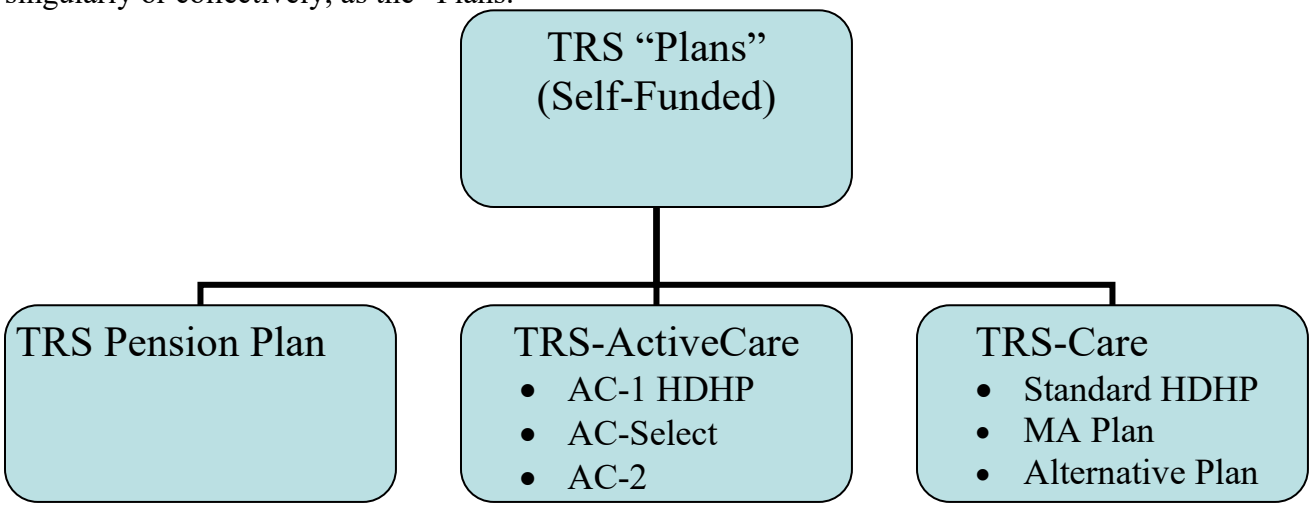
Effective: November 1, 2019

TABLE OF CONTENTS

INTRODUCTION

HIPAA is the responsibility of everyone at the Teacher Retirement System of Texas ("TRS") who uses, discloses or maintains Protected Health Information ("PHI"). This document provides the Privacy Policies and Procedures for compliance with 45 C.F.R. Parts 160, 162, and 164 ("HIPAA Regulations") and Texas Gov't Code § 825.507 for the secure management of PHI. In general, provisions of Code § 825.507 that are contrary to the HIPAA Regulations are preempted by the HIPAA Regulations, and the HIPAA Regulations will apply. If the provisions of Code § 825.507 are more stringent than the HIPAA Regulations, Code § 825.507 will apply. For purposes of this paragraph, "contrary" means: (1) a Covered Entity or Business Associate would find it impossible to comply with both the State and Federal requirements; or (2) the provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of the Administrative Simplification Provisions of HIPAA. In general, a State law is "more stringent" than the HIPAA Regulations if it relates to the privacy of individually identifiable health information and provides greater privacy protections for individuals' identifiable health information, greater rights to individuals with respect to that information, or greater reporting obligations than the HIPAA Regulations do. See 45 C.F.R. 160.202 for more information. These Privacy Policies and Procedures should be read in conjunction with the TRS Security Policies and Procedures.

TRS administers three trust funds for the benefit of active and retired public school teachers in the State of Texas: (a) the Pension Trust Fund; (b) the TRS-ActiveCare Trust Fund; and (c) the TRS-Care Trust Fund. The Pension Trust Fund provides retirement benefits and death benefits to eligible retirees, including benefits based on a member's disability. PHI may be disclosed in the course of providing benefits from the Pension Trust Fund, including disability retirement determinations and review of springing Powers of Attorney (POA). TRS-ActiveCare provides medical and prescription drug benefits to eligible active public school employees and their eligible dependents; these employees must be employed by participating entities in TRS-ActiveCare. TRS-Care provides medical and prescription drug benefits to eligible retirees and their eligible dependents; these retirees have been employed by public school districts and charter schools in the State of Texas during their teaching careers. Each of these programs and their respective trust funds will be referred to in these Privacy Policies and Procedures, whether singularly or collectively, as the "Plans."



TRS will be referred to as the Plan Sponsor in these Privacy Policies and Procedures. The vast majority of PHI associated with the operations of TRS-Care and TRS-ActiveCare is handled by the Third-Party Administrators and Pharmacy Benefit Managers of the Plans.

The Plan Sponsor and the Plans designate themselves as a single Covered Entity for purposes of HIPAA Regulations compliance. Due to the integrated nature of providing benefits under the Plans to TRS members, active employees, and retirees, TRS made the determination to treat all Health Information maintained by all three Plans as PHI under the HIPAA Regulations. As a result, these Privacy Policies and Procedures apply to the PHI held by all three Plans. These Policies and Procedures do not apply to information that is not Health Information or PHI. The TRS Information Security Manual (ISM) provides guidance for the privacy and security of information that is not PHI. Except where necessary to provide integrated service to TRS members, active employees, and retirees, or where otherwise provided in these Privacy Policies and Procedures, PHI associated with one of the Plans should be used solely in connection with that Plan.

Terms used, but not otherwise defined, in these Privacy Policies and Procedures have the meanings set forth in the Glossary located at the end of this document and in the HIPAA Regulations. TRS reserves the right to change these Privacy Policies and Procedures at any time and will review these Privacy Policies and Procedures no less frequently than every two years.

Contacting the Plans' Privacy Officer: The Privacy Officer is Clarke Howard, Assistant General Counsel, TRS Legal & Compliance. He may be contacted at (512) 542-6524, or clarke.howard@trs.texas.gov. Questions on these Privacy Policies and Procedures may also be directed to the Chief Compliance Officer, Heather Traeger. She may be contacted at (512) 542-6884.

POLICY & PROCEDURE FOR ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS FOR PHI

Purpose

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

References

Reference: 45 C.F.R §164.530(c)

Policy

It is the policy of the Plans to address compliance with the HIPAA Regulations by having in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI from an intentional or unintentional use or disclosure that is in violation of the HIPAA Regulations. It is also the policy of the Plans 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 Plans 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 Treatment, Payment or Health Care Operations purposes.

      (iii) If possible, telephone conversations should be conducted away from public areas (*e.g.*, hallways, bathrooms, cafeteria, kitchen, etc.).

(iv) Speakerphones should be used only in private areas.

(v) Verify the identity and authority of the individual making the request according to the Plans' Policy and Procedure for Verification of Individual's Identity and Authority (page 43).

(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) Employees must program the fax machine auto-dial with frequently used numbers to reduce errors in dialing.

(iv) Employees must verify non-routine fax numbers and confirm the receipt of a fax to a non-routine fax number. A fax number is non-routine if it is used for a special reason rather than daily, weekly, or monthly. Employees must double-check the number that has been dialed into the fax machine, before sending the fax.

(v) Employees are to auto-print transmission reports to document where the fax was sent.

(vi) The fax machine header must be set with the correct date, time, and name of facility or office.

(vii) "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.

(viii) Unclaimed items must be shredded regularly after a set time period after confirming materials are not needed.

(ix) 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.

(x) If a fax containing PHI is sent in error: the sender must notify the Privacy Officer.

(xi) Fax machines are to be located in secure areas not readily accessible to visitors.

(xii) 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, and fax number) and an appropriate confidentiality notice.

(c) E-Mail Communications

As a standard policy, TRS does not usually correspond with members through email about PHI. In the exceptional case that we are communicating with a member, employees must follow the security measures below.

(i) When transmitting PHI electronically through email, confirm that the only included email addresses are for the intended recipient(s) by obtaining manager or peer review.

(ii) External email must be sent using encryption by selecting the "Send Securely" option.

(iii) Avoid the use of Social Security numbers and use the unique system-assigned ID instead. This precaution should also be used with internal email, even though internal email is automatically encrypted. An internal email could be forwarded externally, which could possibly result in a breach under HIPAA.

(iv) If an email 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 the person who received the email, name of entity sending the information, phone number and the name of person that was notified, and any return or destroy instructions from them must be logged, and then contact IT Security to delete the email from the system.

(d) Mail Communication

(i) Any PHI that is mailed must be in a sealed envelope.

(ii) Any PHI mailed must be sent via first class, express mail, or other similar service.

(iii) Confirm that the PHI is being mailed to the correct address. Compare the name and address on the documents and envelope against the TRS system.

(iv) Be careful to not include another participant's information in the mailing.

(v) Use non-window envelopes if confidential information is visible through the window.

(e) 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 that contain PHI must be personally shredded in a crosscut shredder or placed in secured shredder bins. TRS will receive confirmation that shredding has occurred.

(iv) Electronic media must be destroyed in accordance with the HIPAA Security Policies and Procedures (the "Security Policies and Procedures") and the Information Security Manual ISM.

2. Technical Safeguards. The Plans will implement and observe technical safeguards through the adoption and use of the attached Security Policies and Procedures and shall apply such Security Policies and Procedures to ePHI maintained by the Plans, as applicable.

3. Physical Safeguards. Physical safeguards that the Plans 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 an unauthorized person when the work area is attended.

(c) Paper records containing PHI must be secured when a workstation is unattended.

(d) Individuals who are not TRS employees or non-TRS workers must be appropriately escorted and monitored when in areas containing 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 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 or lock their computer station at the end of each day. The computer session must be locked when it is left unattended. Employees must log off computer stations when done working on a computer station that is not assigned to them.

4. Privacy Officer Review. The Privacy Officer, the Chief Compliance Officer and Information Security Officer will coordinate to periodically assess and update the safeguards in place.

POLICY & PROCEDURE FOR NOTICE OF PRIVACY PRACTICES, COMPLAINTS, AND PRIVACY OFFICER

Purpose

The HIPAA Regulations provide individuals with the right to receive notice of the Plans' uses and disclosures of their PHI, their individual rights, and the Plans' legal duties with respect to the PHI. They also require the Plans to provide a means for individuals to lodge complaints about the Plans' uses and disclosures of their PHI. They also require the Plans to appoint a Privacy Officer to serve as the individual charged with developing and managing the implementation of the Plans' Privacy Policies and Procedures.

References

Reference: 45 C.F.R §164.520(c)(1)(b)
Reference: 45 C.F.R §164.520(c)(1)(v)
Reference: 45 C.F.R §164.520(c)
Reference: 45 C.F.R §164.520(c)(v)(a)
Reference: 45 C.F.R §164.520(c)(1)(b)
Reference: 45 C.F.R §164.520(c)(1)(iii)
Reference: 45 C.F.R §164.520(c)(1)(iv)
Reference: 45 C.F.R §164.520(c)(3)
Reference: 45 C.F.R §164.520(e) and §164.530(j)
Reference: 45 C.F.R §164.530(d)(1)
Reference: 45 C.F.R §164.530(d)(2)
Reference: 45 C.F.R §164.530(g)
Reference: 45 C.F.R §164.530(a)

Policy

The Plans will provide notice to all its members of the ways that the Plans will use and disclose their PHI and their individual rights as required by the HIPAA Regulations and will provide a means for individuals to lodge complaints and obtain additional information about the uses and disclosures of their PHI. The Plans will also appoint a Privacy Officer who shall have the responsibility of managing and implementing the Plans' Privacy Policies and Procedures, in coordination with the Chief Compliance Officer.

Procedure

1. Timing and Content of Notice. The Privacy Officer will approve the Plans' Notice of Privacy Practices ("Notice") that will be provided:

   (a) at the time that an individual (i) becomes a new member of the Pension Fund, (ii) becomes a new enrollee in TRS-Care or TRS-ActiveCare, (iii) applies for disability retirement; or (iv) submits PHI to evidence the activation of a springing POA; and

   (b) within 60 days of a material revision to the Notice, to individuals then covered by the Plans.

The Privacy Officer shall ensure that the Notice contains all of the elements required by the HIPAA Regulations. For this purpose, the Privacy Officer may use a model notice issued by HHS.

2. New Enrollees. New members in the Pension Plan and new enrollees in the TRS-ActiveCare or TRS-Care Plans will receive the Notice in their initial packets, and as applicable, along with their summary Plan description booklets and other initial notices. Members in the Pension Plan will also receive the Notice when applying for disability retirement benefits and when activating a springing POA.

3. Updates. No less frequently than once every three years, the Plans will notify individuals then covered by the Plans of the availability of the Notice and how to obtain the Notice. The Plans currently notifies individuals on an annual basis.

   If there is a material change to the Notice:

   (a) If the Plans post the 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 Plans.

   (b) If the Plans do not post the 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 Plans within 60 days of the material revision to the Notice.

4. One Notice Per Family. The Plans will provide the Notice to the employee who is enrolled in the Plans and will not provide a separate notice to any dependents of the employees who are also covered by the Plans, unless a Notice is specifically requested by any such dependent.

5. Single Notice For All Coverage Options. The Plans will provide the same Notice to all members, regardless of which benefit program or coverage level in which the member is enrolled.

6. Web Site. The Plans maintain a web site that provides information about the Plans' benefits and prominently posts the Plans' Notice on that web site and makes 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 Plans 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 Plans have a current copy of the Plans' Notice and, through the Business Associate

Agreement, 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 Plans by completing **Form 6 (Complaint Form for Violation of Privacy Rights)** and submitting it to the Plans' Privacy Officer. TRS will investigate and respond to all complaints filed. The Plans' Notice of Privacy Practices will notify individuals of this right, as well as the right to file a complaint with the Secretary of HHS. The Privacy Officer, in coordination with the Chief Compliance 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 Plans, nor TRS, shall retaliate against any individual who lodges a complaint under this Policy and Procedure.

10. Privacy Officer. The Privacy Officer shall be selected by TRS in its role as administrator of the Plans. The Privacy Officer, in coordination with the Chief Compliance Officer, will coordinate the development and implementation of the Plans' Privacy Policies and Procedures. TRS Compliance, in coordination with the Privacy Officer, will have the primary responsibility to manage, regularly monitor, and maintain compliance with these Privacy Policies and Procedures and the requirements of the HIPAA Regulations. The Privacy Officer shall have all duties set forth in these Privacy Policies and Procedures.

    In addition, the Privacy Officer shall:

    (a) Serve as the designated Plans' liaison to regulatory and accrediting bodies and trade associations for matters relating to privacy and security.

    (b) Coordinate, in consultation with the Chief Compliance Officer and Information Security Officer, any response to complaints or compliance reviews for governmental or accrediting organizations concerning the Plans' compliance with state or federal privacy laws or regulations.

    (c) Maintain current knowledge of applicable federal and state privacy and security laws based on bulletins, updates, and other guidance.

    (d) Evaluate, in coordination with the Chief Compliance Officer and the Information Security Officer, the selection, implementation, and administration of Plans privacy and security controls, including new privacy and security technologies as they become available.

    At this time, TRS has designated Clarke Howard as the Privacy Officer. These Privacy Policies and Procedures, including this designation, will be retained by TRS for at least six years.

POLICY & PROCEDURE ON USES & DISCLOSURES WITHOUT CONSENT AND GENETIC INFORMATION

Purpose

The HIPAA Regulations allow the Plans to use or disclose PHI for Treatment activities, Payment activities, and Health Care Operations without the explicit written consent of an individual; however, the HIPAA Regulations allow for the Plans to obtain such a consent if it chooses to do so. In addition, the use and disclosure of Genetic Information is limited.

References

Reference: 45 C.F.R §164.506(a)
Reference: 45 C.F.R §164.502(a)(5)(i)

Policy

The Plans will use or disclose PHI for Treatment activities, 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 Plans' own Payment activities or Health Care Operations, or the Health Care Operations of any other Covered Entity that participates with the Plans in an Organized Health Care Arrangement;

2. for Treatment activities of a Health Care Provider;

3. to obtain bids from vendors that will provide health coverage services under the Plans;

4. to the Medical Board;

5. to another Health Plans, Health Care Clearinghouse, or Health Care Provider for Payment activities of the entity that receives the information; or

6. to another Health Plans, Health Care Clearinghouse, or Health Care Provider for Health Care Operations activities of the entity that receives the PHI if both the Plans and the receiving entity has a relationship with the individual who is the subject of the PHI and the information is used for purposes of detection of fraud and abuse or health care compliance, or for one or more of the following Health Care Operations:

    (a) Conducting quality assessment and improvement activities (including outcomes evaluation and development of clinical guidelines), provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;

    (b) Patient Safety Activities;

    (c) Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of

Health Care Providers and patients with information about Treatment alternatives, and related functions that do not involve Treatment;

(d) Reviewing the competence or qualifications of health care professionals;

(e) Evaluating practitioner performance or Health Plans performance;

(f) Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as Health Care Providers;

(g) Training of non-health care professionals; and

(h) Accreditation, certification, licensing, or credentialing activities.

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 Plans' Policies and Procedures and in particular, the Plans' Policy and Procedure for the Minimum Necessary Requirement (page 40) and for Verification of Individual's Identity and Authority (page 43).

2. Inquiries. Any questions regarding whether a particular use or disclosure of PHI is permissible under this Policy should be directed to the Plans' Privacy Officer. In the Privacy Officer's absence, such questions may be directed to the Chief Compliance Officer, or their designee.

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 & Procedure on Written Authorizations;

   (b) Policy & Procedure on Disclosures to Spouses, Family, and Others;

   (c) Policy & Procedure on Public Policy Uses and Disclosures;

   (d) Policy & Procedure on Disclosures to Business Associates;

   (e) Policy & Procedure for Limited Data Set;

   (f) Policy & Procedure for De-Identification;

   (g) Policy & Procedure on Disclosures of PHI to Plan Sponsor or Employer; and

   (h) Policy & Procedure for an Individual's Right to Request to Inspect and Obtain a Copy of PHI.

4. Special Rule for Genetic Information. The Plans will not use an individual's Genetic Information, including information about an individual or an individual's family

member's genetic tests or genetic conditions, information about an individual's family history, or information regarding the receipt of genetic counseling or other genetic services, for purposes of Health Care Operations related to underwriting, or for purposes of Plans' eligibility. In this context, underwriting means: (a) rules for or determination of eligibility (including enrollment and continued eligibility) for or determination of benefits under the Plans (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (b) the computation of premiums or contribution amounts under the Plans (including discounts, rebates, Payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (c) the application of any pre-existing condition exclusion under the Plans; and (d) other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. Underwriting does not include determinations of medical appropriateness where an individual seeks a benefit under the Plans.

POLICY & PROCEDURE ON WRITTEN AUTHORIZATIONS

Purpose

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

References

Reference: 45 C.F.R §164.508(c)(1)
Reference: 45 C.F.R §164.508(c)(2)
Reference: 45 C.F.R §164.508(b)(4)(ii)
Reference: 45 C.F.R §164.508(b)(2)
Reference: 45 C.F.R §164.508(b)(3)
Reference: 45 C.F.R §164.508(c)(4)
Reference: 45 C.F.R §164.508(a)(3)
Reference: 45 C.F.R §164.508(a)(4)

Policy

1. The Plans will require an authorization to use or disclose PHI if that use or disclosure of PHI is not otherwise permitted without an authorization by the HIPAA Regulations or these Privacy Policies and Procedures.

2. The Plans may use or disclose PHI without an authorization for the following purposes:

   (a) For Treatment activities, Payment activities, or Health Care Operations (as set forth in the Policy & Procedure on Uses and Disclosures without Consent);

   (b) Pursuant to a verbal agreement with an individual (as set forth in the Policy & Procedure on Disclosures to Spouses, Family, and Others);

   (c) For any "public policy" purpose (identified in the Policy & Procedure on Public Policy Uses and Disclosures); 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 Plans' Third-Party Administrators, Pharmacy Benefit Managers, or the Privacy Officer, depending upon which entity is in possession of the PHI.

Procedure

1. General Authorization Forms. If the Plans need 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. A properly completed **Form 1 (Request to Inspect and Copy Health Information)**, Form 628 (Authorization for Use or Disclosure of Protected Health Information), or the Texas Attorney General Form hb300 (Authorization to Disclose Protected Health Information), may be used for this purpose. In addition, any form adopted by the Plans' Third-Party Administrators or Pharmacy Benefit Managers may constitute a valid authorization if it contains the elements in paragraphs 3 and 4 below.

2. Review and Approval of Authorization. The Plans' Privacy Officer will review all authorization forms submitted to TRS prior to any use or 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 Plans may make the requested disclosure;

   (d) A description of each purpose of the requested use or disclosure (however, 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 and the signature date. 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 Plans' Third-Party Administrators, Pharmacy Benefit Managers, 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.

   If the authorization form references information held by a Third-Party Administrator or Pharmacy Benefit Manager, the requestor will be provided contact information and directed to contact the appropriate Third-Party Administrator or Pharmacy Benefit Manager.

3. Required Provisions. The Plans' authorization form contains certain required provisions placing the individual on notice of his or her rights. If the Privacy Officer, Third-Party Administrator, or Pharmacy Benefit Manager receives an authorization form to disclose PHI that was not created by the Plans, the Third-Party Administrator, Pharmacy Benefit Manager or Privacy Officer will verify that that form contains the required elements in item 2 prior to disclosing information pursuant to such form, 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 Plans to condition Payment, enrollment, or eligibility for benefits on the authorization by stating either:

      (i) The Plans 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 Plans can condition enrollment or eligibility for benefits on the individual's signing of the authorization (see paragraph 5 below for times when the Plans may impose conditions).

   (c) A statement that information disclosed pursuant to the authorization may potentially be subject to disclosure by the party receiving the information and may no longer be protected by state or federal privacy laws.

4. When Authorization May Be Required by the Plans. The Plans may condition enrollment in the Plans' programs or eligibility for benefits on the provision of an authorization requested by the Plans prior to an individual's enrollment if that authorization is for the purpose of eligibility or enrollment decisions relating to the individual or the Plans' underwriting or risk rating (so long as the authorization does not apply to Psychotherapy Notes).

5. Revoking Authorizations. The Plans and the Vendors will allow individuals to revoke an authorization in writing at any time. If the Plans have 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 Plans will retain any signed authorization forms for at least six years from the later of the date they were created or last in effect. The Plans will require the Third-Party Administrators and Pharmacy Benefit Managers to retain authorization forms in compliance with this paragraph.

7. Invalid Authorizations. The Privacy Officer, Third-Party Administrators, or Pharmacy Benefit Managers 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 the Plans know the expiration event has passed);

   (b) The authorization has not been filled out completely;

   (c) The Plans know the authorization has been revoked;

   (d) The authorization conditions the Payment, enrollment in the Plans, or eligibility for benefits upon providing the authorization;

   (e) The Plans know 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, except as follows:

   (a) An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study;

   (b) An authorization for a use or disclosure of Psychotherapy Notes may only be combined with another authorization for a use or disclosure of Psychotherapy Notes; and

   (c) An authorization, other than an authorization for the use or disclosure of Psychotherapy Notes, may be combined with any other such authorization, except when the Plans have conditioned the provision of Treatment, Payment, and enrollment in the Plans or eligibility for benefit on the provision of one of the authorizations.

9. Copies to Individuals. If the Plans have requested an authorization from an individual for its own purposes, the Plans will provide the individual with a copy of the signed authorization. In all other instances, the Plans will provide the individual with a copy of the signed authorization upon request.

10. Disclosures to Spouses and Parents. The Plans recognize that spouses and parents sometimes seek the disclosure of their spouses' and non-minor dependent's PHI for purposes of tracking health claims and resolving claims disputes. If the Plans are unable to disclose PHI to a spouse or parent after applying the criteria set forth in Policy & Procedure on Disclosures to Spouses, Family, and Others, the Plans will require an authorization from the spouse or non-minor dependent whose PHI is to be disclosed. **Form 628 (Authorization for Use and Disclosure of Protected Health Information) may be used for this purpose**. Notwithstanding this provision, limited information related to claims status and Payment history may be disclosed to the primary enrollee in the Plans without such an authorization, provided that such information does not include

any information related to the health services or medical conditions associated with the claim.

11. Marketing. The Plans must obtain an authorization for any use or disclosure of PHI for marketing (see Policy & Procedure for Fundraising, Marketing and Sale of PHI) unless the communication is in the form of: (a) a face-to-face communication made by the Plans to an individual; or (b) a promotional gift of nominal value provided by the Plans. If the marketing involves Financial Remuneration to the Plans from a third party, the authorization must state that the Plans are receiving Financial Remuneration for the use or disclosure of the PHI. **At the current time, TRS does not use or disclose PHI for marketing.**

12. Sale of PHI. The Plans must obtain an authorization for any disclosure of PHI that is a sale of PHI. The authorization must state that the disclosure will result in Financial Remuneration to the Plans. **At the current time, TRS does not disclose PHI for the purpose of selling such PHI.**

POLICY & PROCEDURE ON DISCLOSURES TO SPOUSES, FAMILY, AND OTHERS

Purpose

The HIPAA Regulations allow the Plans 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.

References

Reference: 45 C.F.R §164.510(b) (i) and (ii)
Reference: 45 C.F.R §164.510(b)(3)
Reference: 45 C.F.R §164.510(b) (3) (ii)
Reference: 45 C.F.R §164.510(b) (1) and (3)
Reference: 45 C.F.R §164.510(b) (1) (I)
Reference: 45 C.F.R §164.510(b)
Reference: 45 C.F.R §164.502(f)

Policy

1. The Plans will generally not disclose an individual's PHI to the individual's spouse, parent (if the individual is a non-minor dependent) or any other person involved in an individual's care, unless the Plans first obtain a written authorization form or a verbal agreement from the individual whose PHI is to be disclosed. However, the Plans may disclose PHI to family members or people involved in an individual's care or Payment for care in emergency situations, under other circumstances approved by the Privacy Officer, or as otherwise provided in this Procedure, if the Plans first:

   (a) Inform 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, determines in the exercise of professional judgment that the disclosure is in the individual's best interest.

2. The Plans 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 Plans first:

   (a) Inform 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, determines, in the exercise of professional judgment, that the disclosure is in the individual's best interest.

(c) If the individual is deceased, determines, in the exercise of professional judgment, the disclosure is in the individual's best interest and is not inconsistent with any prior expressed preference of the individual as known to the Plans.

3. This Policy will apply to disclosures to spouses and 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, Dependent Children, and Deceased Individuals for special rules that will apply to dependents under age 18.

Procedure

1. Spouses, Family Members & Others (Individual is present). If the Plans receive a request to disclose an individual's PHI to that individual's spouse, parent (if the individual is a non-minor dependent) or any other person involved in the individual's care, and the individual is present, the individual must consent to the disclosure. The individual may consent by submitting an authorization or by verbal agreement. Verbal agreements will only be valid if given during a telephone call or meeting and shall only be valid through the end of the telephone call or meeting if provided in person.

2. Spouses, Family Members & Others (Individual not present). If the Plans receive a request to disclose an individual's PHI to that individual's spouse, parent (if the individual is a non-minor dependent), or any other person involved in the individual's care, and the individual is not present, the Plans may not disclose the PHI unless the standards of paragraph 5 (Individual Incapacitated or Emergency Situation) below are met. In addition, the Plans may release limited claims-related information about spouses and non-minor dependents to the Plans' 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. Any other request for disclosure of an individual's PHI by an individual's 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.

3. Notification. The Plans 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 Plans make 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 incapacitated, or if any emergency exists, the Privacy Officer may determine, in the exercise of professional judgment, the disclosure is in the individual's best interest.

4. Disaster Relief. The Plans 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 the uses or disclosures permitted by paragraph 2 above with such entities. The Plans (through the Privacy Officer) will provide individuals with an opportunity to object to

such disclosures, unless doing so would interfere with the Plans' or other entity's need to respond to the emergency circumstance.

5. Individual Incapacitated or Emergency Situation. If the Plans cannot provide the individual with an opportunity to object because the individual is incapacitated, or there is an emergency situation, any request for a disclosure of the individual's PHI will be handled by the Plans' Third-Party Administrators, Pharmacy Benefit Managers or the Privacy Officer. The Third-Party Administrators, Pharmacy Benefit Managers, or the Privacy Officer 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 Third-Party Administrators, Pharmacy Benefit Managers, 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.

6. Deceased Individual. Disclosure to spouses, family member or friends of a deceased individual's PHI shall be made in accordance with paragraph 3 of the Privacy Policy & Procedure for Personal Representatives, Dependent Children, and Deceased Individuals.

POLICY & PROCEDURE FOR PERSONAL REPRESENTATIVES, DEPENDENT CHILDREN, AND DECEASED INDIVIDUALS

Purpose

The HIPAA Regulations provide that 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. The Plans will recognize a person as a personal representative with respect to PHI relevant to such personal representation if a person has authority to act on behalf of an individual who is an adult, an emancipated minor, an unemancipated minor, or a deceased individual in making decisions related to health care, in accordance with this policy.

References

Reference: 45 C.F.R §164.502(g)(2)
Reference: 45 C.F.R §164.502(g)(3)(i)
Reference: 45 C.F.R §164.502(g)(3)(i)A,B,C
Reference: 45 C.F.R §164.502(g)(5)
Reference: 45 C.F.R §164.502(f)
Reference: 45 C.F.R §164.502(g)(4)

Policy

General Rules. The Plans 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 Plans:

1. Adults & Dependents Age 18 and Over. The Plans 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 Plans receive legal documentation indicating otherwise.

2. Parents, Guardians, & Persons Acting *in loco parentis*. Except as set forth below, the Plans will presume that all custodial parents have the authority to act on behalf of their dependents who are under the age of 18. The Plans will require legal documentation that a non-custodial parent or a non-parent individual is serving as the minor's guardian or in some other legal capacity for the minor before the Plans 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 custodial parents or the appropriate legal documentation.

3. Dependents under Age 18. The Plans will allow dependents under age 18 to act on their own behalf in limited circumstances.

4. Personal Representatives. Except as set forth below, the Plans 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 Plans will first verify the identity and authority of the individual making the request according to the Plans' Policy and Procedure for Verification of Individual's Identity and Authority (page 43).

2. Special Circumstances. After verifying the individual's identity and authority, the Plans 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 Plans 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, such as when a court may consent in lieu of a parent or guardian (*e.g.*, drug and alcohol abuse Treatment and Treatment for sexually transmitted diseases),

      (ii) the PHI relates to medical Treatment that was provided to the minor under confidential circumstances and the Plans are made aware of such confidential circumstances, or

      (iii) the parent or guardian agreed to confidentiality between a Health Care Provider and the minor regarding a health care service and the Plans are made aware of such agreement.

   (b) Personal Representatives for any Individual (Including Dependents under Age 18). The Plans may elect not to treat a person as the personal representative of an individual if:

      (i) the Plans have 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 Plans' Third-Party Administrators, Pharmacy Benefit Managers, or the Privacy Officer decide in the exercise of professional judgment 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 Plans 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. If no executor or administrator has been appointed, the Plans may disclose a deceased individual's PHI to a family member, relative, or close personal friend involved in the health care or Payment for health care of the individual, and authorized to act on behalf of the individual at the

time of death, if based on the exercise of professional judgment of the Plans' Third-Party Administrators, Pharmacy Benefit Managers or the Privacy Officer, that the disclosure would be in the individual's best interests. The Plans will not make such disclosure if it determines that doing so is inconsistent with any prior express preference of the individual as known to the Plans. Information is no longer considered PHI once an individual has been deceased for 50 years.

4. Confidential Communications. Any individual may request that the Plans **not** treat another person as his or her personal representative by completing **Form 3 (Request for Confidential Communications)** and submitting it to the Plans' Third-Party Administrators, Pharmacy Benefit Managers or the Privacy Officer.

POLICY & PROCEDURE ON PUBLIC POLICY USES AND DISCLOSURES

Purpose

The HIPAA Regulations allow the Plans 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 & Procedure.

References

Reference: 45 C.F.R §164.512(b)
Reference: 45 C.F.R §164.512(f)
Reference: 45 C.F.R §164.512(c)
Reference: 45 C.F.R §164.512(d)
Reference: 45 C.F.R §164.512(g)
Reference: 45 C.F.R §164.512(h)
Reference: 45 C.F.R §164.512(k)
Reference: 45 C.F.R §164.512(i)
Reference: 45 C.F.R §164.512(l)
Reference: 45 C.F.R §164.512(e)(1)
Reference: 45 C.F.R §164.512(e)(ii)(a)
Reference: 45 C.F.R §164.512(e)(iii)
Reference: 45 C.F.R §164.512(e)(ii)(b)
Reference: 45 C.F.R §164.512(e)(iv-v)
Reference: 45 C.F.R §164.512(c)(2)

Policy

1. Permitted. The Plans will use and disclose PHI for certain public policy reasons without obtaining the individual's authorization as allowed in the HIPAA Regulations and set forth below:

   (a) As Required By Law; or

   (b) In response to any court or administrative order issued in the course of a judicial or administrative proceeding (including, but not limited to a qualified medical child support order).

2. Non-Routine Disclosures. Although the HIPAA Regulations allow the Plans to use or disclose PHI without the individual's permission for other public policy purposes, the Plans do not anticipate the need to do so. Therefore, the Plans will not routinely make the following uses or disclosures of PHI, unless Required By Law or in exceptional circumstances as approved by the Privacy Officer:

   (a) for any public health or law enforcement purpose;

   (b) about an individual whom the Plans believe to be a victim of abuse, neglect, or domestic violence to a government authority (such as social services or protective services);

(c) to a Health Oversight Agency for oversight activities;

(d) to a coroner or medical examiner;

(e) for organ procurement or other organizations for purposes of facilitating organ, eye, or tissue donation or transplantation;

(f) to prevent or lessen a serious and imminent threat to health or safety;

(g) for specialized government functions;

(h) for research purposes; or

(i) to comply with laws related to workers' compensation or similar employer-related programs.

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, excluding Qualified Medical Child Support Orders (QMCSO), the Plans will forward the request to TRS Legal and Compliance for legal review prior to making any disclosure. The QMCSO procedure is provided in 2 below.

   (a) Court and Administrative Orders. TRS Legal and Compliance will verify the validity of the order and advise the Plans as to whether the requested disclosure may be made. If the order is valid, TRS Legal & Compliance 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 Plans (through TRS Legal and Compliance in consultation with the Privacy Officer) shall take reasonable and appropriate steps to notify the court or administrative body that issued the order of the Plans' objections to releasing the PHI.

   (b) Subpoenas, Discovery, and Other Legal Process. TRS Legal and Compliance 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 Plans. 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 Plans 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 Plans 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 Plans 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 Plans by the party seeking the disclosure. Neither the Plans, nor TRS Legal and Compliance, 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. Qualified Medical Child Support Order (QMCSO). The Office of the Attorney General (OAG) electronically mails the National Medical Support Notice (NMSN) to TRS Payroll and Benefits Department P&B. P&B reviews the NMSN to determine if it applies to a TRS employee. When the individual is a TRS employee, P&B responds to the NMSN via online reporting. P&B forwards all other NMSNs to the Plans' NMSN Administrator in the Health and Insurance Benefits Division (HIB) for review and processing. Unless the individual is an employee of a participating entity, the Plans' NMSN Administrator respond to the NMSN by mailing the hardcopy of the Plans' response to the OAG. When the individual is an employee of a participating entity in TRS-ActiveCare, the Plans' NMSN Administrator will (1) generate a transmittal cover letter, and then send the original documents received from the OAG to the Employer; and (2) retain one set of copies in the TRS files. It is the responsibility of the Employer to respond to the OAG.

3. Other Disclosures Required By Law. Upon receipt of any request for the Plans to disclose PHI for any of the other public policy purposes listed above, or upon receipt of any request for the Plans to disclose PHI due to any legal requirement, the Plans will forward the request to TRS Legal and Compliance for legal review prior to making the disclosure.

4. Non-Routine Disclosures. Any request for a non-routine disclosure identified in paragraph 3 of the Policy section of this Policy and Procedure shall be referred immediately to the Privacy Officer. The Privacy Officer shall determine whether such disclosures should be made consistent with the HIPAA Regulations. The Privacy Officer shall approve such disclosures only in rare and exceptional circumstances which shall be determined in the Privacy Officer's sole discretion, although the Privacy Officer may consult with TRS Legal & Compliance prior to making the disclosure. If the disclosure is made, the Privacy Officer will promptly inform the individual whose PHI is being disclosed that such a report has been or will be made in accordance with the HIPAA Regulations.

5. Logging Disclosures. All disclosures made pursuant to this Policy must be reported to the Plans' Privacy Officer who will log the disclosure.

POLICY & PROCEDURE FOR LIMITED DATA SET

Purpose

The HIPAA Regulations allow the Plans 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.

References

Reference: 45 C.F.R §164.514(e)(1)
Reference: 45 C.F.R §164.514(e)(3)
Reference: 45 C.F.R §164.514(e)(4)(ii)
Reference: 45 C.F.R §164.514(e)(2)
Reference: 45 C.F.R §164.514(e)(4)(iii)

Policy

1. The Plans may use or disclose a limited data set for purposes of research, public health activities, or Health Care Operations, if the Plans enter into a data use agreement with the limited data set recipient.

2. The Plans 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 Plans.

Procedure

1. Identification of Need for Data Use Agreements. The Plans' Privacy Officer will review any request for use of a limited data set and any potential limited data set recipients, 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 Plans' Privacy Officer will advise TRS employees and non-TRS workers and others who perform services on behalf of the Plans as to any identified limited data set recipient who has not executed and returned the requested data use agreement, and employees or service providers will not disclose a limited data set to any such entity.

3. Contents of Agreement. A data use agreement between the Plans 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 HIPAA Regulations if done so by the Plans;

(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 Plans 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 Plans' Privacy Officer and may only be executed by the Plans' 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 Plans 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. If such steps are unsuccessful, the Privacy Officer shall ensure that:

(a) disclosures of PHI to the recipient are discontinued; and

(b) the problem is reported to the Secretary of HHS.

7. Reporting Violations. Determinations of whether disclosures will be discontinued or problems reported to the Secretary of HHS shall be made by the Plans' Privacy Officer in consultation with the Chief Compliance Officer.

POLICY & PROCEDURE ON DISCLOSURE OF PHI TO THE PLAN SPONSOR OR EMPLOYER

Purpose

The HIPAA Regulations allow the Plans to disclose PHI to the Plan Sponsor or Employer, for Plans' administration functions if certain protective steps are implemented. The Plans will allow these disclosures consistent with this Policy & Procedure.

References

Reference: 45 C.F.R §164.314
Reference: 45 C.F.R §164.504

Policy

1. The Plans will disclose an individual's PHI to the Plan Sponsor to carry out Plans' administration functions, as described in the Policy & Procedure for Minimum Necessary Requirement. For these purposes, "Plans' administration functions" means administrative functions performed by the PHI Employees on behalf of the Plans, and excludes functions performed by the Plan Sponsor in connection with any other benefit or benefit plans of the Plan Sponsor, or in the Plan Sponsor's role as an employer.

2. The Plans will disclose to the Plan Sponsor or Employer information on whether the individual is participating in TRS-Care or TRS-ActiveCare, or is enrolled in or has disenrolled from a plan offered under TRS-Care or TRS-ActiveCare, including a plan offered by an HMO that is associated with either of these two programs.

3. The Plans may disclose Summary Health Information to the Plan Sponsor or Employer.

4. Before the Plan discloses PHI to the Plan Sponsor or Employer, the Plan will follow the procedures set forth below.

Procedure

1. Requirements for Disclosure to Plan Sponsor. If the Plans receive a request to disclose an individual's PHI to the Plan Sponsor, the Plans will ensure that the Plans' documents has been amended as provided in paragraph 2 below.

2. Plan Amendments. Before the Plans disclose PHI to the Plan Sponsor for Plans' administration functions, the Plans' documents must be amended to incorporate provisions to:

   (a) establish the permitted and required uses and disclosures of such information by the Plan Sponsor or Employer;

   (b) provide that the Plans will disclose PHI to the Plan Sponsor or Employer only upon receipt of a certification by the Plan Sponsor or Employer that the Plans have been

amended to incorporate the following provisions and the Plan Sponsor or Employer has agreed to:

(i) not use or further disclose PHI other than as permitted or required by the Plans or as Required By Law;

(ii) ensure that any agents, including subcontractors, to which the Plan Sponsor or Employer provides PHI received from the Plans, agree to the same restrictions and conditions that apply to the Plan Sponsor or Employer;

(iii) not use or disclose PHI for employment-related actions and decisions;

(iv) not use or disclose PHI in connection with any other benefit or employee benefit plans of the Plan Sponsor or Employer;

(v) report to the Plans any use or disclosure of PHI inconsistent with the HIPAA Regulations' requirements of which the Plan Sponsor or Employer becomes aware;

(vi) make PHI available to an individual pursuant to the HIPAA Regulations' access requirements at 45 CFR §164.524;

(vii) make PHI available for amendment, and incorporate any PHI amendments in accordance with the HIPAA Regulations at 45 CFR §164.526;

(viii) make available the information required to provide an accounting of disclosures in accordance with the HIPAA Regulations at 45 CFR §164.528;

(ix) make available to the Secretary of HHS the Plan Sponsor's or Employer's internal practices, books and records relating to the use and disclosure of PHI received from the Plans to determine the Plans' compliance with the HIPAA Regulations;

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

3. Uses and Disclosures. The Plans may:

   (a) disclose PHI to the Plan Sponsor or Employer to carry out Plans' administration functions only as is consistent with this Policy & Procedure;

   (b) not permit a Health Insurance Issuer or HMO with respect to the Plans to disclose PHI to the Plan Sponsor or Employer except as permitted by this Policy & Procedure;

   (c) not disclose or permit a Health Insurance Issuer or HMO to disclose PHI to the Plan Sponsor or Employer as otherwise permitted by this Policy & Procedure unless a separate statement to that effect is included in the appropriate notice of privacy practices; and

   (d) not disclose PHI to the Plan Sponsor or Employer for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plans of the Plan Sponsor or Employer.

4. Summary Health Information. The Plans may disclose Summary Health Information to the Plan Sponsor or Employer without regard to paragraphs 1-3 of this Procedure if the Plan Sponsor or Employer requests the Summary Health Information for the purpose of: (a) obtaining premium bids from Health Plans for providing health insurance coverage under the Plans; or (b) modifying, amending, or terminating the Plans. For these purposes, "Summary Health Information" means information that may be Individually Identifiable Health Information that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom the Plan Sponsor has provided health benefits under the Plans, and from which the data elements listed in paragraph 2 of the Policy and Procedure on De-Identification (page 45) have been removed (except that the geographic information need only be aggregated to the level of a five-digit zip code).

POLICY & PROCEDURE ON DISCLOSURES TO BUSINESS ASSOCIATES

Purpose

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

References

Reference: 45 C.F.R §164.502(e)(1)
Reference: 45 C.F.R §164.504(e)(2)
Reference: 45 C.F.R §164.504(e)(4)(i-ii)

Policy

1. The Plans will identify those Business Associates that create, receive, maintain, or transmit PHI of Plans members and beneficiaries in order to perform services for the Plans.

2. The Plans will obtain satisfactory assurance that its Business Associates will appropriately safeguard PHI disclosed to, created, 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:

   (a) disclosures by the Plans to Health Care Providers concerning the Treatment of an individual; or

   (b) certain disclosures by the Plans to the Plan Sponsor or Employer as allowed under the HIPAA 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 Plans:

   (a) creates, receives, maintains, or transmits PHI for a function or activity regulated by the HIPAA Regulations; or

   (b) provides legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services to or for the Plans where the provision of the service involves the disclosure of PHI from the Plans.

Procedure

1. Coordination with Other Policies: See Security Policies & Procedures.

2. Identification of Business Associates. The Plans' Procurement and Contract's Team (P&C), with the assistance of the Business Unit and L&C, will identify all potential Business Associates of the Plans, send a "Business Associate Agreement" to each Business Associate identified, and oversee the execution and timely return of those contracts. All amendments, updates and changes in scope of existing contracts will be reviewed by P&C to determine if a Business Associate Agreement is required.

3. Subcontractors of Business Associates. The Plans are not required to obtain agreements with subcontractors of the Plans' Business Associates. The Plans' Business Associates shall be required to obtain satisfactory assurance that its subcontractors will appropriately safeguard PHI disclosed to, created by, or received by its subcontractors. Such satisfactory assurance shall be in the form of a written contract.

4. Effect of No Agreement. The Plans' Privacy Officer will advise TRS employees, non-TRS workers and others who perform any service on behalf of the Plans as to any identified Business Associates who have not executed and returned the Business Associate Agreement. In the absence of a Business Associate Agreement, PHI will not be provided to the identified entities unless the data is provided in accordance with the Privacy Policy and Procedure for Limited Data Set.

5. Contents of Agreements. The Plans' Business Associate Agreements will at a minimum:

    (a) establish the permitted and required uses and disclosures of PHI by the Business Associate;

    (b) include a copy of the Plans' Notice of Privacy Practices;

    (c) permit the Business Associate to provide Data Aggregation services relating to the Health Care Operations of the Plans; and

    (d) 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, disclosure, or request for PHI to the minimum amount 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 HIPAA Regulations, including with respect to electronic PHI;

        (iv) report to the Plans any use or disclosure of the PHI not provided for under the contract, including Breaches of Unsecured PHI (see Policy &

Procedure for Securing PHI and Notification in Case of Breach of Unsecured PHI);

(v) ensure that any agents or subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate on behalf of the Plans 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 Plans can satisfy its access, amendment, and accounting obligations to individuals;

(vii) to the extent the Business Associate is to carry out the Plans' obligations under the HIPAA Regulations, comply with the requirements of the HIPAA Regulations that apply to the Plans 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 Plans' compliance with the HIPAA Regulations;

(ix) at termination of the contract, if feasible, return or destroy all PHI received from, created, or received by the Business Associate on behalf of the Plans 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 Plans, if the Plans determine that the Business Associate has violated a material term of the contract.

(xi) 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.

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

Section 5, such as requiring indemnification from a Business Associate in the event its acts result in liability for the Plans.

6. Violations of Agreements. The Plans' 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, TRS shall terminate the Business Associate Agreement and any underlying agreement or relationship with the Business Associate, if reasonably feasible.

7. Documentation. P&C shall maintain copies of each Business Associate Agreement for at least 75 years after the contract's final term ends.

POLICY & PROCEDURE FOR FUNDRAISING, MARKETING AND SALE OF PHI

Purpose

The HIPAA Regulations allow the Plans to use PHI for marketing purposes with an individual's authorization and limited sets of PHI for the purpose of raising funds. The sale of PHI is prohibited and the Plans may not receive any direct or indirect remuneration in exchange for PHI. **Notwithstanding the existence of this Policy, at the current time TRS does not use or disclose PHI for marketing purposes.**

References

Reference: 45 C.F.R §164.514(f)

Policy

1. The Plans will not use or disclose PHI for the purpose of fundraising or marketing, nor will it receive any indirect or direct remuneration for any PHI.

2. Prior authorization is required for all Treatment and Health Care Operations communication where the Plans receives Financial Remuneration for making such communications from a third party whose product or service is being marketed.

3. Marketing does not include communications made by the Plans to describe a health-related product or service (or Payment for such product or service) that is provided by, or included in a Plans of benefits of, the Plans. Therefore, the Plans may use and disclose PHI without the individual's authorization to communicate with individuals about entities participating in a health care provider network or Health Plans network, about replacement of or enhancements to the benefits offered by the Plans, and other health related products or services available only to the Plans' members, and for case management or care coordination for the individual. Marketing also does not include communication by the Plans to provide refill reminders. Such uses and disclosures are subject to the Privacy Policy & Procedure on Uses & Disclosures Without Consent and Genetic Information.

4. Marketing further does not include any communications made by the Plans as described under paragraph 2 above for which the Plans receive or has received direct or indirect Payment in exchange for making such communications under the following circumstances:

    (a) Where such communication provides refill reminders or otherwise communicates about or describes only a drug or biologic that is currently being prescribed for the recipient of the communication, and any Payment received by the Plans in exchange for making such communication is reasonable in amount; or

(b) Where such communication is made by the Plans and the Plans obtain from the recipient of the communication a valid authorization; or

(c) Where such communication is made by a Business Associate on behalf of the Plans and the communication is consistent with the Business Associate Agreement.

5. The Plans will not sell any PHI or otherwise receive any direct or indirect remuneration in exchange for PHI. The sale of PHI occurs where the Plans or a Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. The following circumstances are *not* considered to be the sale of PHI and are *not* prohibited by the Plans' policy against selling PHI or receiving direct or indirect remuneration in exchange for PHI:

(a) The purpose of the exchange is for public health activities as defined in 45 C.F.R. §164.512(b) or (e);

(b) The purpose of the exchange is for research, as defined in 45 C.F.R. §§164.501, 164.512(i), 164.514(e), where the only remuneration received by the Plans or Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;

(c) The purpose of the exchange is for Treatment or Payment purposes pursuant to 45 C.F.R. §164.506(a);

(d) The purpose of the exchange is for the sale, transfer, merger, or consolidation of all or part of the Plans or Plan Sponsor and for related due diligence as described in 45 C.F.R. §164.501(6)(iv) and pursuant to 45 C.F.R. §164.506(a);

(e) The purpose of the exchange is to or by a Business Associate for activities undertaken on behalf of a Plans or on behalf of the Business Associate in the case of a subcontractor, and the only remuneration provided is by the Plans to the Business Associate, or by the Business Associate to a subcontractor, if applicable, for the performance of such activities;

(f) The purpose of the exchange is to provide an individual with a copy of his PHI pursuant to a valid request; or

(g) The purpose of the exchange is Required By Law as permitted under 45 C.F.R. §164.512(a); and

(h) The purpose of the exchange is for any other purpose permitted by and in accordance with the applicable requirements of the HIPAA Regulations, where the only remuneration received by the Plans or a Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

Procedure

Any requests for the use or disclosure of PHI for fundraising or marketing purposes, or for the sale of PHI, shall be directed to the Privacy Officer who shall deny such requests.

POLICY & PROCEDURE FOR MINIMUM NECESSARY REQUIREMENT

Purpose

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

References

Reference: 45 C.F.R §164.514(d)
Reference: 45 C.F.R §164.514(d)(1)(b)(2)
Reference: 45 C.F.R §164.514(d)(2)
Reference: 45 C.F.R §164.514(d)(4)
Reference: 45 C.F.R §164.514(d)(3)(i)
Reference: 45 C.F.R §164.514(d)(5)
Reference: 45 C.F.R §164.514(d)(3)(iii)

Policy

1. When using or disclosing PHI, or when requesting PHI from another Covered Entity (Health Care Provider, Health Plans, or Health Care Clearinghouse), the Plans 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 HHS issues guidance on what constitutes "minimum necessary," the Plans 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 Plans, 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 & Procedure for Limited Data Set (page 27).

2. Exceptions to the minimum necessary requirement include:

   (a) disclosures to or requests by a Health Care Provider for Treatment;

   (b) uses or disclosures made to the individual who is the subject of the information;

   (c) uses or disclosures made pursuant to an authorization;

   (d) disclosures made to the Secretary of HHS pursuant to a privacy investigation;

   (e) uses and disclosures that are Required By Law; and

   (f) uses or disclosures that are required by the HIPAA Regulations or other laws.

3. Employees who perform services on behalf of the Plans will be trained to apply the minimum necessary principle to the use and disclosure of PHI.

Procedure

1. Identification of Persons Who Need Access. The Privacy Officer, Chief Health Care Officer, and the Chief Benefits Officer have identified certain TRS employees or non-TRS workers who need access to PHI to carry out their essential job duties (the "PHI employees"). Access shall be granted in accordance with Section 4 of the Security Policies and Procedures. The Privacy Officer may designate other individuals to use PHI. These employees or non-TRS workers receive training consistent with the Policy and Procedure for Employee Training and Corrective Actions in the use and disclosure of PHI. A list of PHI employees is available from IT Security and Compliance.

2. Requests to Others. When requesting information from other entities, such as Health Plans or medical providers, the Plans 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 Plans identify routine and recurring requests that it makes of others for PHI, the Plans 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. At this time, TRS has not identified any such requests.

4. Entire Record. The Plans may not use, disclose or request an entire medical, claims, or 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 or trained employees and non-TRS workers 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 HIPAA 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 TRS employee or non-TRS worker or is a Business Associate of the Plans for the purpose of providing professional services to the Plans, 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 HIPAA Regulations have been provided by a person requesting the information for research purposes.

6. De-Identified Information. Whenever possible, the Plans should use and disclose only de-identified information (see Policy & Procedure for De-Identification), 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.

7. TRS Employee Information. Access to current TRS Member-Employee information is generally assigned to a couple of employees in each department. TRS employee records are flagged as sensitive data. IT Security monitors unauthorized access to TRS Member/Employee information by generating and reviewing a Sensitive Data Access Report (SDAR). The SDAR is provided to managers on a monthly basis for confirmation of authorization.

POLICY & PROCEDURE FOR VERIFICATION OF INDIVIDUAL'S IDENTITY AND AUTHORITY

Purpose

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

References

Reference: 45 C.F.R §164.514(h)(2)(i)
Reference: 45 C.F.R §164.514(h)(2)(ii)
Reference: 45 C.F.R §164.514(h)(2)(iii)

Policy

Prior to any disclosure of PHI, the Plans must verify the authority and identity of the individual to whom the disclosure is to be made. The verification requirements are met if the Plans exercise professional judgment in using or disclosing PHI in accordance with the Policy and Procedure on Disclosures to Spouses, Family, and Others 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 Plans will verify the individual's identity (if the person acting on behalf of the Plans 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.

    (c) The Plans may verify additional data elements, if additional verification is needed.

2. Documents. When a disclosure is conditioned on particular documentation, statements, or representations from the person making the request, the Plans 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 Plans 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 Plans 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 Plans 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 instrument issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

POLICY & PROCEDURE FOR DE-IDENTIFICATION

Purpose

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

References

Reference: 45 C.F.R §164.514(b)(1)
Reference: 45 C.F.R §164.514(b)(2)
Reference: 45 C.F.R §164.514(c)

Policy

PHI is Individually Identifiable Health Information or Genetic Information that is transmitted or maintained by TRS. 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, not PHI, and may be use without limitation under the HIPAA Regulations. However, uses and disclosures of this information may still be prohibited by other applicable state or federal laws or regulations. The de-identified information will only be used if the Plans do 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 Plans 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 Plans may assign a code or other means of record identification to allow information that has been de-identified to be re-identified by the Plans, 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 Plans do 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 TRS Reports. From time to time, the Plans may need to disclose de-identified or aggregate information to appropriate TRS 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.

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 Plans (including, but not limited to, the Plans' Business Associates) without the prior approval of the Privacy Officer.

POLICY & PROCEDURE FOR AN INDIVIDUAL'S RIGHT TO REQUEST RESTRICTIONS

Purpose

The HIPAA 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 their care or Payment for care. The Plans are not Required By Law to agree with such requests. However, if the Plans do agree, the PHI will be restricted as to use and disclosure, unless an emergency situation requiring such information's use or disclosure arises.

References

Reference: 45 C.F.R §164.522(a)(1)
Reference: 45 C.F.R §164.522(a)(1)(iii)
Reference: 45 C.F.R §164.522(a)(1)(vi)
Reference: 45 C.F.R §164.522(a)(2)
Reference: 45 C.F.R §164.522(a)(3)

Policy

1. The Plans will permit an individual to request that the Plans restrict the uses and/or disclosures of an individual's PHI in the following ways:

   (a) to carry out Treatment activities, 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 care or Payment for care.

2. The Plans are not required to agree to a request for restrictions, except as provided below.

3. If the Plans agree to the request for a restriction, the Plans 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 Plans' 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 Plans' Third-Party Administrators or Pharmacy Benefit Managers that complies with the HIPAA Regulations), or obtain from the TRS website.

2. If Restrictions Are Granted. If the Plans agree 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 Plans' TRS employees and non-TRS workers and the Plans' Third-Party Administrators or Pharmacy Benefit Managers as to the restriction.

3. Required Restriction. The Plans 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 Plans on behalf of the individual, has paid the Plans 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. Emergency Treatment. If restricted PHI needs to be disclosed to a Health Care Provider for emergency Treatment purposes the Plans may disclose the PHI, but the Plans will request that such Health Care Provider not further use or disclose the information.

5. Continued Use. Even if the Plans have agreed to a restriction, the Plans 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 Plans' Policy and Procedure on Public Policy Uses and Disclosures; or

(d) to the Secretary of HHS to investigate or determine the Plans' compliance with the HIPAA Regulations.

6. Terminating Restrictions. The Plans 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 Plans inform the individual that the Plans are terminating the agreement, except that such termination is only effective with respect to PHI created or received after it has so informed the individual.

7. Documentation. When the Plans agree to a restriction, the Business Unit shall document the restriction 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. The Privacy Officer shall keep a log of the requested restrictions.

8. Records Held by the Plans' Service Providers. If the Plans' Privacy Officer receives any request for restrictions as to the use or disclosure of information that may be maintained by the Plans' service providers (such as the Plans' Third-Party Administrators or Pharmacy Benefits Managers), the Privacy Officer will inform such service providers of the request. The Privacy Officer shall consult with the affected service provider to determine the degree to which the service provider can comply with the requests. Based upon these discussions, and in light of degree to which the Plans themselves are willing to comply with the request, the Plans will determine the response to the request and inform the service provider of the same.

   The Plans 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 Plans.

   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 Plans pursuant to a service provider's standard policies and procedures that are consistent with these Privacy Policies and Procedures and the HIPAA Regulations.

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

Purpose

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

References

Reference: 45 C.F.R §164.524(a)
Reference: 45 C.F.R §164.524(b)
Reference: 45 C.F.R §164.524(c)
Reference: 45 C.F.R §164.524(c)(3)
Reference: 45 C.F.R §164.524(c)(4)
Reference: 45 C.F.R §164.524(d)
Reference: 45 C.F.R §164.524(d)(2)
Reference: 45 C.F.R §164.524(d)(3)
Reference: 45 C.F.R §164.524(e)

Policy

1. An individual has a right of access to inspect and obtain a copy of their own PHI maintained by the Plans in a Designated Record Set. This right does not apply to:

   (a) Psychotherapy Notes;

   (b) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; or

   (c) PHI maintained by the Plans that is subject to the Clinical Laboratory Improvements Amendments of 1988, to the extent the provision of access to the individual would be prohibited by law or exempt from the Clinical Laboratory Improvements Amendments of 1988.

2. The Plans 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 HIPAA Regulations do not require the Plans 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.

3. The Plans may deny an individual access to his or her own PHI, subject to providing the individual an opportunity for review of that decision if:

   (a) a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

   (b) the PHI makes reference to another person (unless such other person is a Health Care Provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

   (c) the request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

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)** to the Business Unit. Individuals may obtain the form from the TRS website or by contacting TRS.

2. Designated Record Set. The Plans 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, claims adjudication, and case medical management records systems maintained by the Plans, or any other group of records used by the Plans to make decisions about the individual.

3. Timing of Response. The Plans will act on an access request no later than 30 days after receipt of the request, unless the Plans are unable to take action on the request within 30 days and follows the procedures for extension of time, found in paragraph 5 below.

4. Records Held by the Plans Service Providers. If the Plans' Privacy Officer receives any request for information that may be maintained by the Plans' service providers (such as the Plans' Third-Party Administrators or Pharmacy Benefit Managers), the Privacy Officer, by contract or otherwise, will direct the requestor to the appropriate service providers and allow the service providers to independently respond to a request with regard to PHI maintained by such service provider on behalf of the Plans pursuant to the service provider's standard policies and procedures that are consistent with these Privacy Policies and Procedures and the HIPAA Regulations. The Plans 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 Plans 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.

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

   (a) the Plans, within the initial time for responding, provide the individual with a written statement of the reasons for the delay and the date by which the Plans will complete its action on the request; and

   (b) the Plans may have only one such extension of time for action on a request for access.

6. If Access Is Granted. If the Plans (either directly or through its Third-Party Administrator or Pharmacy Benefit Manager) grant the access request, in whole or in part:

   (a) the Plans will provide the access requested within a timely manner;

   (b) the Plans 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 Plans 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 Plans and the individual;

   (d) if the information is maintained electronically, the Plans will provide the information in the form and format requested by the individual if the information is readily producible; or, if the information is not readily producible, the Plans must provide the information in a readable electronic form as agreed to by the individual and the Plans;

   (e) the Plans 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 Plans for such summary or explanation;

   (f) the Plans 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 Plans 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 Plans 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, the summary, or the explanation be mailed; and

(iv) preparing an explanation or summary of the PHI, if agreed to by the individual.

If the Plans' Privacy Officer receives any request for electronic information to be forwarded to a designated third party, the Plans 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. Form 628 (Authorization for Use or Disclosure of Protected Health Information) may be used for this purpose.

7. If Access Is Denied. If the Plans (either directly or through its Third-Party Administrator or Pharmacy Benefit Manager) deny access, in whole or in part:

(a) the Plans will, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI as to which the Plans have reason to deny access;

(b) the Plans 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 Plans or to the Secretary of HHS, including the name, or title, and telephone number of the contact person or office responsible to receive complaints;

(c) if the Plans do not maintain the PHI that is the subject of the individual's request for access, and the Plans know where the requested information is maintained, the Plans will inform the individual where to direct the request for access; and

(d) if the individual has requested a review of a denial, the Plans 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 Plans 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 Plans will promptly provide written notice to the individual of the determination made by the designated reviewing official.

8. Documentation. The Plans 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 & PROCEDURE FOR AN INDIVIDUAL'S RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

Purpose

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

References

Reference: 45 C.F.R §164.522(b)(1)(i)
Reference: 45 C.F.R §164.522(b)(1)(ii)
Reference: 45 C.F.R §164.522(b)(2)

Policy

1. The Plans will permit individuals to request to receive communications of PHI from the Plans by alternative means or at alternative locations other than the addresses identified in their Plans records.

2. If the individual clearly states that the disclosure of all or part of his or her PHI could endanger the individual, then subject to other terms of this Privacy Policy and Procedure, the Plans will accommodate all reasonable requests on an as needed basis.

3. Individuals who are not endangered may request immediate transmission of available documents. However, these individuals may not request temporary or short-term communication changes, or request alternative mailing addresses in addition to their permanent address.

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 Plans' Third-Party Administrators or Pharmacy Benefit Managers that complies with the HIPAA Regulations) to the Plans' Privacy Officer. Individuals may obtain the form from the TRS website or by contacting the Privacy Officer.

2. Conditions. The Plans 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 Plans 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 Business Unit 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 Plans' Third-Party

Administrators or Pharmacy Benefit Managers) and forward the instructions accordingly. The Plans shall use the alternative means of communication until the individual submits a new request pursuant to this Policy.

5. Records Held by the Plans' Service Providers. If the Plans' Privacy Officer receives any request for confidential communications as to information that may be maintained by the Plans' service providers (such as the Plans' Third-Party Administrators or Pharmacy Benefits Managers), the Privacy Officer will inform such service providers of the request. The Privacy Officer shall consult with the affected service provider to determine the degree to which the service provider can comply with the requests. Based upon these discussions, and in light of degree to which the Plans themselves are willing to comply with the request, the Plans will determine the response to the request and inform the service provider of the same.

   The Plans 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 Plans.

   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 Plans pursuant to a service provider's standard policies and procedures that are consistent with these Privacy Policies and Procedures and the HIPAA Regulations.

6. Documentation. If the Plans agree to a request for confidential communications pursuant to this Policy, the Compliance Department shall maintain documentation of its agreement to grant the request for at least six years after the Plans' agreement is no longer in effect.

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

Purpose

The HIPAA 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 Plans maintain it within a Designated Record Set.

References

Reference: 45 C.F.R §164.526(a)(1)
Reference: 45 C.F.R §164.526(a)(2)
Reference: 45 C.F.R §164.526(c)
Reference: 45 C.F.R §164.526(d)

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 Plans.

2. The Plans 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 Plans, 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 HIPAA Regulations and the Plans' Policy & Procedure for an Individual's Right to Request to Inspect and Obtain a Copy of PHI; or

   (d) is accurate and complete.

Procedure

1. To Request An Amendment. All requests that the Plans 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 Plans' Third-Party Administrators or Pharmacy Benefit Managers that complies with the HIPAA Regulations) and submitted to the Plans' Privacy Officer. All requests must provide a reason to support a requested amendment. Individuals may obtain the form from the TRS website or by contacting the Privacy Officer.

2. Amendment Permitted. If the Plans grant 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 Plans (or was created by someone who is no longer available to act on the request amendment); and

   (b) maintained in a "Designated Record Set."

3. Amendment Denied. The Plans will deny an individual's request to amend if the PHI:

   (a) was not created by the Plans, 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 HIPAA Regulations and the Plans' Policy & Procedure for an Individual's Right to Request to Inspect and Obtain a Copy of PHI (page 51); or

   (d) is accurate and complete.

4. Timing of Response. The Plans (through the Privacy Officer) will respond to any amendment request within 60 days of receipt if possible. Otherwise, the Plans may extend the time for such action by no more than 30 days, provided that:

   (a) within the original 60 day time period, the Plans provide the individual with a written statement of the reasons for the delay and the date by which the Plans will complete its action on the request; and

   (b) the Plans may have only one such extension of time for action on a request for an amendment.

5. If the Request Is Granted:

   (a) the Plans 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 Plans 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 Plans know 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 that 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 Plans 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 Plans or to the Secretary of HHS, 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 Plans may reasonably limit the length of a statement of disagreement;

(c) the Plans 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 Plans' denial of the request, the individual's statement of disagreement, if any, and the Plans' rebuttal, if any, to the Designated Record Set; and

(e) upon the Plans' denial of an amendment, future disclosures, require the following:

(i) if a statement of disagreement has been submitted by the individual, the Plans will include the material appended, or, at the election of the Plans, 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 Plans 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 Plans may separately transmit the material to the recipient of the standard transaction.

7. Amendments By Others. If the Plans are informed by another Covered Entity of an amendment to an individual's PHI, the Plans will amend PHI within a Designated Record Set of the Plans and the Privacy Officer will inform any of the Plans' service providers (such as the Plans' Third-Party Administrators or Pharmacy Benefit Managers) who maintain affected PHI in a Designated Record Set of the amendment and cause them to make the amendment.

8. Records Held by the Plans' Service Providers. If the Plans' Privacy Officer receives any request to amend an individual's information that may be maintained by the Plans' service providers (such as the Plans' Third-Party Administrators or Pharmacy Benefits Managers), the Privacy Officer will inform such service providers of the request. The Privacy Officer shall consult with the affected service provider to determine the degree to which the service provider can comply with the requests. Based upon these discussions, and in light of degree to which the Plans themselves are willing to comply with the request, the Plans will determine the response to the request and inform the service provider of the same.

   The Plans shall require its service providers to forward to the Privacy Officer any requests for amendment that they receive directly from individuals for a decision by the Plans.

   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 Plans pursuant to a service provider's standard policies and procedures that are consistent with these Privacy Policies and Procedures and the HIPAA Regulations.

9. Documentation. If TRS maintains the applicable documents, the Privacy Officer 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.

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

Purpose

The HIPAA Regulations provides individuals with the right to request an accounting of certain disclosures made by TRS, acting in its capacity as administrator of the Plans, of an individual's Protected Health Information ("PHI").

References

Reference: 45 C.F.R §164.528(a)
Reference: 45 C.F.R §164.528(a)(1)
Reference: 45 C.F.R §164.528(b)(2)
Reference: 45 C.F.R §164.528(b)(3)
Reference: 45 C.F.R §164.528(c)
Reference: 45 C.F.R §164.528(c)(2)
Reference: 45 C.F.R §164.528(d)
Reference: 45 C.F.R §164.528(a)(2)

Policy

1. An individual has a right to receive an accounting of certain disclosures of PHI made by TRS 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 HIPAA Regulations or these Privacy Policies and Procedures (including inadvertent or mistaken disclosure);

   (b) any disclosures TRS makes pursuant to a public policy purpose as set forth in these Privacy Policies and Procedures;

   (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. TRS need not provide an accounting of the following types of disclosures of PHI:

   (a) to carry out Treatment, 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 HIPAA Regulations;

   (d) pursuant to an authorization;

(e) for national security or intelligence purposes;

(f) to correctional institutions or Law Enforcement Officials related thereto;

(g) as part of a limited data set; or

(h) that occurred prior to April 14, 2004.

Procedure

1. To Request an Accounting. To request an accounting of disclosures of PHI, an individual must submit a request in writing to the TRS Privacy Officer on **Form 5 (Request for an Accounting of Disclosures)**. Individuals may obtain the form from the TRS website or by contacting the Privacy Officer.

2. Logging Disclosures. In order to comply with this accounting obligation, TRS Compliance 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 Plans 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 Agreements, shall cause service providers (i) that provide services on behalf of the Plans and (ii) that have access to PHI from the Plans (Business Associates, as that term is set forth in the glossary) to maintain records that comply with the HIPAA Regulations and to report accountable disclosures to the Privacy Officer or to an individual when requested.

3. Information Provided in Accounting. The Disclosure Log and any written accounting provided by TRS 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; 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, TRS has made multiple disclosures of PHI to the same person or entity for a single purpose related to disclosures to the Secretary of HHS or for public policy reasons recognized in the HIPAA 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. TRS will act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows:

   (a) TRS will provide the individual with the accounting requested; or

   (b) if TRS is unable to provide the accounting within the 60 day period, TRS may extend the time to provide the accounting by no more than 30 days, provided that:

      (i) TRS, within the original 60 day period, provides the individual with a written statement of the reasons for the delay and the date by which TRS will provide the accounting; and

      (ii) TRS may have only one such extension of time for action on a request for an accounting.

6. Charge. TRS will provide the first accounting to an individual in any 12-month period without charge. TRS 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 TRS 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 Privacy Officer 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. TRS 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 TRS 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, TRS 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 Business Associates. If the Privacy Officer receives a request for an accounting of disclosures of an individual's information made by Business Associates, the Privacy Officer, by contract or otherwise, will inform the individual where to direct the request for an accounting to allow a Business Associate to independently respond, on behalf of TRS, to a request with regard to PHI maintained by such Business Associate pursuant to the Business Associate's standard policies and procedures that are consistent with these Privacy Policies and Procedures and the HIPAA Regulations.

POLICY & PROCEDURE FOR SECURING PHI AND ADDRESSING BREACHES

Purpose

The HIPAA Regulations requires the Plans to follow certain notification procedures in the event of a Breach of Unsecured PHI. The Secretary of HHS has issued guidance specifying the technologies and methodologies that render PHI secured. PHI that is not secured in accordance with this guidance is subject to the Breach notification rules described in this Policy.

References

Reference: 45 C.F.R §164.530(j)
Reference: 45 C.F.R §164.530(b)
Reference: 45 C.F.R §164.402
Reference: 45 C.F.R §164.404(a)
Reference: 45 C.F.R §164.404(b)
Reference: 45 C.F.R §164.404(c)(1)
Reference: 45 C.F.R §164.404(d)
Reference: 45 C.F.R §164.406
Reference: 45 C.F.R §164.408
Reference: 45 C.F.R §164.410
Reference: 45 C.F.R §164.412
Reference: 45 C.F.R §164.414(b)

Policy

1. TRS, in its capacity as administrator for the Plans, will endeavor to secure all PHI in accordance with this guidance issued by the Secretary of HHS. Secured PHI is not subject to the Breach notification rules described in this Policy.

2. TRS will implement reasonable internal systems for discovery of Breaches of PHI. This Policy should be read in conjunction with the Security Policies and Procedures for Security Incidents and Breach Notification.

3. Through Business Associate Agreements, TRS will require the service providers (i) that provide services on behalf of the Plans and (ii) that have access to PHI from the Plans (Business Associates, as defined in the glossary), to implement their own reasonable internal systems for discovery of Breaches of PHI, to ensure the timely compliance with all notice requirements in the event of a Breach of Unsecured PHI, and to adhere to agreed upon contractual provisions defining the roles of TRS and the Business Associate in the event of a Breach of Unsecured PHI. The TRS Privacy Officer will also monitor in coordination with P&C and the Contract Sponsor that Business Associates of TRS are contractually required to abide by this Policy.

4. In reviewing whether or not a Breach of PHI has occurred, TRS will conduct a risk assessment and document its determination.

5. 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, TRS will follow the Breach notification procedures, as set forth below.

Procedures

1. Endeavor to Secure All PHI. To the extent practicable, TRS 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, TRS 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, TRS will shred or destroy the media, such that the PHI cannot be read or reconstructed. TRS will not use redaction as a means of data destruction. With respect to electronic media, TRS will clear, purge, or destroy the media consistent with the published guidance from the National Institute of Standards and Technology and in accordance with the Security Policy and Procedure for Device and Media Controls - Disposal and Reuse.

2. 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, in coordination with the Chief Compliance Officer and the Information Security Officer, will be responsible for implementing reasonable internal systems for discovery of Breaches of PHI by TRS, and through Business Associate Agreements, TRS will require its Business Associates to comply with the HIPAA Regulations, which includes the implementation of reasonable internal systems for discovery of Breaches of PHI, to ensure the timely compliance with all notice requirements in the event of a Breach of Unsecured PHI.

   (a) Training. The Chief Compliance Officer will be responsible for ensuring that TRS' employees and non-TRS workers are trained to effectively identify and communicate any discovery of a suspected Breach or a Breach of PHI (whether unsecured or secured), in accordance with the TRS Corrective Action Policy and the Learning and Development Policy.

   (b) Business Associate Agreements. Business Associates are Required By Law to comply with the Breach notification rules under the HIPAA Regulations. In its Business Associate Agreements, TRS will appropriately define the role of TRS and

the Business Associate in the event of a Breach of Unsecured PHI, as described in the Privacy Policy and Procedure on Disclosures to Business Associates.

3. Determination of Breaches and Preliminary Disclosure Report.

(a) Any TRS employee and non-TRS worker who has reason to believe that there may have been an impermissible acquisition, access, use or disclosure by TRS of PHI shall contact the Privacy Officer as soon as reasonably possible, but in no event later than the following business day after the staff member comes into possession of the information that forms the basis of his or her concern about a possible impermissible acquisition, access, use or disclosure of PHI by TRS.

(b) Within fifteen (15) days of receiving the notice described immediately above, the Privacy Officer shall, in coordination with the Chief Compliance Officer and the Information Security Officer, (i) investigate and describe in writing the detailed circumstances of the potential impermissible acquisition, access, use or disclosure, and (ii) make an initial determination regarding whether an impermissible acquisition, access, use or disclosure in fact exists, whether the impermissible acquisition, access, use or disclosure involves any PHI, and if so, determine whether the PHI was "unsecured"[1] or secured (*e.g.*, encrypted). If the Privacy Officer determines that no acquisition, access, use or disclosure in fact exists, or that the acquisition, access, use or disclosure involves no PHI, or that the acquired, accessed, used or disclosed PHI was secured, then no Breach has occurred. The Privacy Officer will reduce this determination to writing in a disclosure report (the "Preliminary Disclosure Report") within 30 business days.

(c) Permitted Uses

If there was an unauthorized acquisition, access, use, or disclosure of unsecured PHI, then within twenty (20) days of receiving the notice described in Item 3(a) above, the Privacy Officer shall determine whether the unauthorized acquisition, access, use, or disclosure was permitted by the HIPAA Regulations.

(i) The Privacy Officer will, in coordination with the Chief Compliance Officer and the Information Security Officer, determine whether the unauthorized acquisition, access, use, or disclosure was limited to the "minimum necessary" for Treatment, Payment and Health Care Operations. If the answer is "yes," then no Breach occurred. If the answer is "no," the analysis must continue.

(ii) The Privacy Officer will, in coordination with the Chief Compliance Officer and the Information Security Officer, determine whether the unauthorized acquisition, access, use, or disclosure was limited to the PHI

[1] "Unsecured" PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in guidance by the Secretary of HHS.

that was encrypted, destroyed or properly de-identified (limited data set with no identifiers and does not include dates of birth or zip codes). If the answer is "yes," then no Breach occurred. If the answer is "no," the analysis must continue.

(d) Exception to Definition of Breach

If there was an unauthorized acquisition, access, use, or disclosure of unsecured PHI, then within twenty (20) days of receiving the notice described in Item 3 (a) above, the Privacy Officer shall determine whether the unauthorized acquisition, access, use, or disclosure falls into an exception to the definition of a Breach.

(i) The Privacy Officer will, in coordination with the Chief Compliance Officer and the Information Security Officer, determine: (a) whether the unauthorized acquisition, access, use, or disclosure was unintentional and done by a TRS employee and non-TRS worker or person acting under the authority of TRS; and (b) whether it was 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 did not result in further use or disclosure in a manner not permitted under the HIPAA Regulations. If the answer to all of these is "yes," then no Breach occurred. If the answer to any of these is "no," the analysis must continue.

(ii) The Privacy Officer will, in coordination with the Chief Compliance Officer and the Information Security Officer, determine: (a) whether the unauthorized acquisition, access, use, or disclosure was an inadvertent disclosure by a person who is authorized to access PHI by TRS to another person authorized to access PHI at TRS; 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 HIPAA Regulations. If the answer to both of these is "yes," then no Breach occurred. If the answer to either of these is "no," the analysis must continue.

(iii) The Privacy Officer will, in coordination with the Chief Compliance Officer and the Information Security Officer, 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 the answer is "yes," then no Breach occurred. If the answer is "no," the analysis must continue.

If the unauthorized acquisition, access, use, or disclosure of unsecured PHI does not fall into a permitted use or an exception to the definition of a Breach, then within the same twenty (20) day period of receiving the notice described in Item 3(a) above, using all relevant details available, the Privacy Officer shall document that determination in the Preliminary Disclosure Report, and prepare a risk assessment (the "Risk Assessment"). In completing the Risk Assessment, the Privacy Officer will, in coordination with the Chief Compliance Officer and the

Information Security Officer, determine whether the impermissible use or disclosure amounts to a Breach.

4. Risk Assessment

An impermissible acquisition, access, 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 TRS demonstrates that there is a low probability that the PHI has not been compromised based upon the Risk Assessment, using four factors.

The four factors of the Risk Assessment include:

(a) 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 (*e.g.*, Treatment plans, diagnosis, medication, medical history information, test results). 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 re-identified based on the context and the ability to link the information with other available information. For example, if the Plans 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 Plans disclosed a list of patient discharge dates and diagnoses, a risk assessment likely would determine that there is only a low probability that any of the individuals could be identified based on the specificity of the diagnosis, the size of the community served by the Plans, 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).

(b) 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 Regulations 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 Plans. 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.

(c) 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 Plans 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.

(d) 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. The Privacy Officer should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised. For example, the Plans 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 the PHI it received in error, while such assurances from certain other third parties may not be sufficient.

5. Notification to Individuals

(a) General Rule. Following the discovery of a Breach of Unsecured PHI, TRS or the Business Associate will notify each individual whose Unsecured PHI has been, or is reasonably believed by TRS or the Business Associate to have been, accessed, acquired, used, or disclosed as a result of such Breach.

(b) Breaches Treated as Discovered. TRS and the Business Associate will treat the date on which a Breach of Unsecured PHI is discovered as the first day that the Breach is known to TRS or the Business Associate, or the first day on which the Breach would have been known to TRS or the Business Associate had they been exercising reasonable diligence.

(c) Timeliness. Except in the case that law enforcement requests a delay, TRS or the Business Associate 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 TRS or the Business Associate. In the case that the Breach is first discovered by a Business Associate of TRS, the Privacy Officer will either (i) confirm that the Business Associate will send out the required notification no later than 60 calendar days after the Business Associate discovered the Breach or (ii) ensure that TRS will send out the required notification no later than 60 calendar days after the Business Associate notifies TRS 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 Plans or the Business Associate 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 Plans or the Business Associate 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 Plans or the Business Associate will send the notification by first-class mail to each such individual's last known address. In the case that the Plans or the Business Associate has insufficient or out-of-date contact information that precludes a written notification, the Plans or the Business Associate may provide a substitute notice, which may be made by telephone if the Plans or the Business Associate has insufficient contact information for fewer than 10 individuals. If the Plans or the Business Associate has insufficient contact information for 10 or more individuals, the Plans or the Business Associate may provide notice through either a conspicuous posting on the Plans' website or the Business Associate'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 Plans or the Business Associate to require urgency, the Plans or the Business Associate 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.

6. Notification to the Media. TRS or the Business Associate 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. TRS or the Business Associate 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.

7. Notification to the Secretary. TRS or the Business Associate will notify the Secretary of HHS (the "Secretary") of Breaches of Unsecured PHI. If the Breach involves 500 or more individuals, TRS or the Business Associate will notify the Secretary within the same timeframe that it provides individual notifications. If the Breach involves fewer than 500 individuals, TRS or the Business Associate 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. TRS or the Business Associate will provide information about any Breaches to the Secretary in the manner specified on the HHS website.

8. Notification by a Business Associate. TRS shall make good faith efforts to require, through its Business Associate Agreements, that:

(a) Each Business Associate shall establish its own reasonable internal systems for the discovery and determination of Breaches of unsecured PHI.

(b) If the Business Associate discovers a Breach of Unsecured PHI, the Business Associate shall promptly notify TRS of the Breach so that the Business Associate or TRS can notify affected individuals. If the Business Associate is responsible for providing such notice, TRS will further require the Business Associate to provide TRS with a copy of such notice. TRS will also require the Business Associate to provide TRS, to the extent possible, with the identification of each affected individual and any other available information.

(c) Similarly, either the Business Associate or TRS shall timely provide notification to the media (if required) and timely provide notification to the Secretary. If the Business Associate is responsible for providing such notices, the Privacy Officer shall take reasonable steps to confirm that timely notice is given by the Business Associate. TRS will further require the Business Associate to provide TRS with a copy of such notice.

(d) The Business Associate Agreements will govern the required actions of the Business Associates in the event of a Breach of Unsecured PHI, and shall specify that all required notifications be made timely, in compliance with the requirements noted above and in compliance with the law.

9. Law Enforcement Delay. The Plans or the Business Associate 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 notify the appropriate Business Associate and will also document (i) the request and (ii) the identity of the official making the statement.

10. Notification to TRS Management. The Privacy Officer shall notify, as soon as reasonably possible, the Executive Director, the Chief Benefits Officer, the Chief Audit Executive, the Chief Health Care Officer, the General Counsel, and the Director of Communications, of any Breaches that involve 500 or more individuals

11. Documentation of Impermissible Uses and Disclosures. TRS and Business Associate, as applicable, have the burden of demonstrating that all required notifications have been made under this Policy, or, alternatively, that a Preliminary Disclosure Report and/or Risk Assessment was conducted and TRS or the Business Associate determined the impermissible use or disclosure did not constitute a Breach of Unsecured PHI, and therefore notifications were not required.

Accordingly, TRS Compliance shall maintain all of the following documentation in compliance with the Records Management Program:

- copies of all written policies and procedures regarding Breach notification;

- copies of applicable, appropriate sanctions against TRS employees and non-TRS workers who do not comply with this Policy and the above-noted procedures;

- copies of all Preliminary Disclosure Reports;

- copies of all Risk Assessments, including the application of any exceptions to the definition of a "Breach" under HIPAA;

- copies of all notifications to individuals, to the media, and to the Secretary of HHS, including copies of the logs of Breaches used in submitting these notifications;

- evidence of training of employees on the above noted policies and procedures

The Privacy Officer shall notify the General Counsel and Chief Compliance Officer of each Preliminary Disclosure Report and Risk Assessment. The Privacy Officer shall then advise the Executive Director, the Chief Benefits Officer, the Chief Audit Executive, the Chief Health Care Officer, and the supervisor of the personnel responsible for the impermissible use or disclosure of the PHI, of these reports and assessments, as appropriate.

POLICY & PROCEDURE FOR EMPLOYEE TRAINING & CORRECTIVE ACTION

Purpose

The HIPAA Regulations require that all TRS employees and non-TRS workers be educated and trained as to the appropriate manner of handling PHI in order to carry out their job functions and that those who fail to comply with the Plans' Privacy Policies and Procedures be appropriately sanctioned.

References

Reference: 45 C.F.R §164.530(b)
Reference: 45 §164.530(b)(2)(ii)
Reference: 45 §164.530(e)(1)

Policy

TRS will train all TRS employees and non-TRS workers on the importance of privacy and TRS' policies and procedures with respect to PHI, as necessary and appropriate for TRS employees and non-TRS workers to carry out their function within the Plans.

Procedure

1. Identifying Trainees and Timing of Training. The Chief Compliance Officer, in coordination with the Information Security Officer and the Privacy Officer, will be responsible for identifying TRS employees and non-TRS workers who perform a function for the Plans involving the use of PHI. The Chief Compliance Officer will ensure that TRS employees and non-TRS workers receive training according to the following schedule:

   (a) to each new TRS employee or non-TRS worker within 30 days after the person joins TRS or is assigned to TRS; and

   (b) to each TRS employee or non-TRS worker 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, and no less frequently than annually.

   The Plans will provide additional training as to the Plans' Policies and Procedures to any individual employee or Business Associate of the Plans, upon request.

2. Content of Training. Training will involve an overview of TRS' obligations under the HIPAA Regulations and the TRS' Policies and Procedures that are applicable to the individuals being trained. The training may be presented in written, electronic, or verbal form.

3. Documentation of Training. Organizational Excellence 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. Corrective Actions. TRS employees and non-TRS workers who use or disclose an individual's PHI in violation of the training provided, the HIPAA Regulations, or these Privacy Policies and Procedures will be subject to corrective actions that will be consistent with the nature of the violation. Consistent with the TRS Corrective Action Policy, action may include, but is not limited to, verbal and written notice, suspensions, and termination. Corrective actions will be imposed by the Executive Director in consultation with the Chief Compliance Officer and Privacy Officer. TRS Compliance will document any sanctions that are imposed.

POLICY & PROCEDURE FOR "WHISTLEBLOWING" AND TRS EMPLOYEE AND NON-TRS WORKER CRIME VICTIMS

Purpose

The Plans respect the privacy of individuals' PHI, but recognizes that information must sometimes be disclosed to avert unlawful conduct or dangerous situations. This Policy describes permissible uses and disclosure of PHI for purposes of averting such situations and informing authorized officials.

References

Reference: 45 C.F.R §164.502(j)(1)
Reference: 45 C.F.R §164.502(j)(2) and §164.512(f)(2)(i)
Reference: 45 C.F.R §164.530(g)
Reference: 45 C.F.R. §160.316

Policy

The Plans, a TRS employee or non-TRS worker providing service to the Plans, or one of the Plans' Business Associates may use PHI or disclose it to appropriate individuals for purposes of reporting certain unlawful conduct or dangerous conditions in accordance with the procedure below.

Procedure

1. Whistleblowing. The Plans, a TRS employee or non-TRS worker, or a Business Associate may disclose PHI without authorization from an individual to whom the information relates in the following circumstances:

   (a) if the TRS employee, non-TRS worker or Business Associate believes in good faith that the Plans have engaged in conduct that is unlawful or otherwise violates professional standards, or that the services provided by the Plans potentially endanger one or more patients, workers, or the public; and

   (b) the disclosure is to:

      (i) a Health Oversight Agency or Public Health Authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Plans or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Plans; or

      (ii) an attorney retained by or on behalf of the TRS employee, non-TRS worker or Business Associate for the purpose of determining the legal options of the TRS employee, non-TRS worker or Business Associate with regard to the conduct described in paragraph 1(a) of this section.

2. Crime Victims. A TRS employee or non-TRS worker who provides service to the Plans and who is the victim of a criminal act may disclose PHI to a Law Enforcement Official if:

(a) the information disclosed is about the suspected perpetrator of the criminal act; and

(b) the information disclosed is limited to the following information:

(i) name and address;

(ii) date and place of birth;

(iii) social security number

(iv) ABO blood type and rh factor;

(v) type of injury;

(vi) date and time of Treatment;

(vii) date and time of death, if applicable; and

(viii) a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

3. Non-Retaliation. TRS shall not retaliate against any individual for filing a complaint; testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing; or opposing any act or practice made unlawful, provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of law.

GLOSSARY

Breach

1. The acquisition, access, use, or disclosure of Protected Health Information in a matter not permitted under the HIPAA 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 TRS employee, a non-TRS worker, 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 HIPAA 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, or Organized Health Care Arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA 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 HIPAA 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 or of an Organized Health Care Arrangement in which the Covered Entity participates, 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 HIPAA 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, or to or for an Organized Health Care Arrangement in which the Covered Entity participates, 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 concerning the Treatment of the individual.

   (b) An employer, 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 employer.

   (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.

(d) A Covered Entity participating in an Organized Health Care Arrangement that performs a function or activity as described by paragraph (1)(a) of this definition for or on behalf of such Organized Health Care Arrangement, or that provides a service as described in paragraph (1)(b) of this definition to or for such Organized Health Care Arrangement by virtue of such activities or services.

Business Unit

A division in TRS that provides a specific business function (such as the Benefits Services Division, the Health and Insurance Benefits Division, and the Investment Management Divisions).

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.

Contract Sponsor

The Executive Officers who have the responsibility for initiating procurement and daily contracting administration within their respective areas of responsibility. Executive Officers may further delegate these responsibilities to their subordinates at the Executive Officer's discretion; however, the Executive Officer retains Contract Sponsor responsibility for all contracts within their respective areas.

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 medical records and billing records about individuals maintained by or for a covered Health Care Provider;

   (b) The enrollment, Payment, claims adjudication, and case or medical management 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.

Employer

A participating entity as defined in section 1579.002(5) of the Texas Insurance Code.

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.

Genetic Information

Genetic Information means:

1. Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

   (a) The individual's genetic tests;

   (b) The genetic tests of family;

   (c) The manifestation of a diseased or disorder in family members of such individual; or

   (d) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

2. Any reference to Genetic Information concerning an individual or family member of an individual shall include the Genetic Information of:

   (a) A fetus carried by the individual or family member who is a pregnant woman; and

   (b) Any embryo legally held by an individual or family utilizing an assisted reproductive technology.

3. Genetic Information excludes information about the sex and age of any individual.

Group Health Plan (also see definition of Health Plans)

A plan 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, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; Patient Safety Activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of Health Care Providers and patients with information about Treatment alternatives; and related functions that do not include Treatment;

2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, Health Plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as Health Care Providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

3. Underwriting, enrollment premium rating, and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the Health Plan receiving Individually Identifiable Health Information does not disclose such information if the insurance or benefits are not placed with it.

4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

5. 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

6. 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, employers, or other customers, provided that PHI is not disclosed to such policy holder, employer, 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;

    (e) Creating de-identified Health Information or a limited data set, and if current policy is amended to allow fundraising, fundraising for the benefit of the Covered Entity; and

(f) Use of an individual's PHI in pension administration in the furtherance of the purpose for which the PHI was provided to the Plans, such as processing an application for disability retirement or reviewing a springing POA.

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.

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.

HIPAA

The Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 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 (IIHI)

Information that is created or received by an employer, a Health Care Provider, a Health Plan, or Health Care Clearinghouse and relates to the past, present, or future physical or mental health or condition of an individual; the provision of Health Care; or the past, present, or future Payment for the provision of health care to an individual; and that identifies the individual, or with respect to which there is reasonable basis to believe the information can be used to identify the individual.

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.

Organized Health Care Arrangement

Any of the following arrangements:

1. A clinically integrated care setting in which individuals typically receive health care from more than one Health Care Provider.

2. An organized system of health care in which more than one Covered Entity participates and in which the participating covered entities:

   (a) Hold themselves out to the public as participating in a joint arrangement; and

   (b) Participate in joint activities that include at least one of the following:

      (i) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

      (ii) Quality assessment and improvement activities, in which Treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

      (iii) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if Protected Health Information created or received by a Covered Entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

3. A Group Health Plan and a Health Insurance Issuer or HMO with respect to such Group Health Plan, but only with respect to Protected Health Information created or received by such Health Insurance Issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such Group Health Plan.

4. A Group Health Plan and one or more other Group Health Plans each of which are maintained by the same Plan Sponsor.

5. The Group Health Plan described in paragraph 4 and Health Insurance Issuers or HMOs with respect to such Group Health Plan, but only with respect to Protected Health Information created or received by such Health Insurance Issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such Group Health Plans.

Participant

A TRS member, former member, retiree, annuitant, beneficiary, alternate payee, program participant (including a health benefit program enrollee), or person eligible for TRS benefits.

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 or subrogation of health benefit claims;

   (b) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

   (c) Billing, claims management, collection activities, obtaining Payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

   (d) Review of health care services with respect to medical necessity, coverage under a Health Plan, appropriateness of care, or justification of charges;

   (e) Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and

   (f) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or 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.

Pharmacy Benefit Manager

A person or entity chosen by the Plans or the Plan Sponsor to assist the Plans with identified administrative functions of prescription drug programs. PBMs are primarily responsible for developing and maintaining the formulary, contracting with pharmacies, negotiating discounts and rebates with drug manufacturers, and processing and paying prescription drug claims. Each Pharmacy Benefit Manager is a Business Associate of the Plans.

Plans

TRS administers three trust funds for the benefit of active and retired public school teachers in the State of Texas: (a) the Pension Trust Fund; (b) the TRS-ActiveCare Trust Fund; and (c) the TRS-Care Trust Fund. The Pension Trust Fund provides retirement benefits and death benefits to eligible retirees, including benefits based on a member's disability. Disability determinations and springing POAs require the use of PHI. TRS-ActiveCare provides medical and prescription

drug benefits to eligible active public school employees and their eligible dependents; these employees must be employed by participating entities in TRS-ActiveCare. TRS-Care provides medical and prescription drug benefits to eligible retirees and their eligible dependents; these retirees have been employed by public school districts and charter schools in the State of Texas during their teaching careers. Each of these programs and their respective trust funds will be referred to in these Privacy Policies and Procedures, whether singularly or collectively, as the "Plans."

Plan Sponsor

Teacher Retirement System of Texas

Protected Health Information or PHI

Individually Identifiable Health Information or Genetic Information that is transmitted or maintained in any form or medium.

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 TRS in its role as employer; and

   (d) Information about an individual who has been deceased for 50 years.

Psychotherapy Notes

Notes recorded (in any medium) by a Health Care Provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy Notes* exclude medication prescription and monitoring,

counseling session start and stop times, the modalities and frequencies of Treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the Treatment plans, symptoms, prognosis, and progress to date.

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 the HHS 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.

Third Party

An entity or individual, including a contractor, who conducts business on behalf of or in cooperation with TRS or provides goods or services to TRS.

Third-Party Administrator

A person or entity chosen by the Plans or the Plan Sponsor to assist the Plans with identified administrative functions in the provision of medical benefit coverage such as claims administration or adjudication. Each *Third-Party Administrator* is a Business Associate of the Plans.

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 HHS in the guidance issued under the HIPAA Regulations.

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.