Rhode Island Laborers' Health & Welfare Fund

HIPAA Privacy Policies & Procedures

Adopted Pursuant to the Privacy Rules Under The Health Insurance Portability and Accountability Act (HIPAA), as Amended by the Health Information Technology for Economic and Clinical Health Act (HITECH)

Effective August 26, 2025

Contents

Introduction

All workforce members who have access to PHI on behalf of the Plan must comply with these policies and procedures for HIPAA privacy compliance. Use of PHI to which workforce members have access is subject to the minimum necessary standard. Workforce members have access to PHI for permitted Plan administrative functions based on their role.

1. Use and disclosure for treatment, payment, and health care operations purposes

Policy

This policy and procedure is adopted by the Rhode Island Laborers Health and Welfare Fund, (Plan) pursuant to Section 164.506 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by HHS, the Plan will follow the revised rules.

PHI may be used and disclosed without authorization for purposes permitted under the HIPAA Privacy Rule. Most importantly, PHI may be used or disclosed without authorization for purposes related to treatment, payment, and health care operations.

Health care treatment purposes include disclosures of PHI if requested by a health care provider.

Health care payment activities include the use and disclosure of PHI for payment activities, such as claims and appeals, claim reimbursement, and other payment activities.

Health care operations use and disclosure activities include:

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; 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, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable. However, the Plan will not use or disclose PHI that is genetic information for underwriting purposes;
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 requirements of this subchapter;
    b. customer service, including the provision of data analyses for policyholders, plan sponsors, other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer;
    c. resolution of internal grievances;
    d. the sale, transfer, merger, or consolidation 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
    f. the plan does not use PHI for fundraising for the benefit of the covered entity.

Organized health care arrangements include relationships between group health plans and their insurers and HMOs. Covered entities participating in an organized health care arrangement may disclose PHI about an individual to another covered entity for any health care operations activities of the organized health care arrangement. Each covered entity is not required to have a relationship with the individual for sharing of PHI as long as it is related to health care operations activities.

2. Minimum necessary

Policy statement

This policy and procedure is adopted pursuant to Section 164.502(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by HHS, the Plan will follow the revised rules.

When using or disclosing PHI, or when requesting PHI from another covered entity, the Plan will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The Plan will make its own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of its business and workforce, and implement policies and procedures accordingly.

Procedures

1. The Plan will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose when using PHI, disclosing PHI, and requesting PHI.
2. The minimum necessary standard applies to oral, electronic, and written PHI.
3. Fund office employees who use and disclose PHI for a use permitted in Section 1 of these Policies and Procedures will be considered to be those within the Plan's workforce who need access to PHI to carry out their job duties. For each person or class of persons, the Plan will identify the category of PHI to which access is needed and any conditions appropriate to such access. See *45 CFR 164.514(d).*
4. The Plan will adopt data security measures designed to protect PHI and limit access as appropriate.
5. Members of the Plan's workforce and any temporary staff or business associates must be trained in the Plan's privacy policies before they may access PHI.
6. Plan staff may only access an individual's PHI when they are working on a payment or health care operation issue involving the individual or his or her dependent(s). For example, staff members cannot view files on which they are not working, unless access is necessary for purposes of assuring consistent and accurate claims administration.
7. Plan staff may not discuss an individual's PHI unless it is necessary to perform a payment or health care operation function. For example, staff should not discuss interesting claims with colleagues who do not have a need to know the information.

Routine disclosures

1. When information is disclosed to the Board of Trustees, the Plan will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose.
2. When receiving a request for PHI from one of the following categories of individuals, the Plan may rely on the judgment of the requestor as to the minimum amount of information that is necessary: However, if the request is vague or overly broad, Plan staff may seek clarification before responding.

a. A public official or agency for a disclosure to them that is permitted under HIPAA
b. A health plan, health care clearinghouse, or health care provider that is covered by the HIPAA rules
c. A business associate

3. Business associate agreements should require a business associate to request from the Plan only the minimum information necessary to perform their functions on behalf of the Plan.

Non-routine disclosures

The Privacy Official or its designee must approve any non-routine disclosures. A non-routine disclosure is a disclosure of PHI that is not addressed by the minimum necessary procedures. Each non-routine disclosure must be reviewed on an individual basis. The criteria for reviewing a non-routine disclosure are as follows:

1. The non-routine disclosure must be necessary (1) to allow the Plan to carry out its obligations under ERISA, HIPAA and/or the governing plan documents, (2) required by law, or (3) pursuant to an individual's authorization.
2. The non-routine disclosure must be limited to the minimum necessary information.
3. The non-routine disclosure must be otherwise consistent with the Plan's privacy policies.
4. The non-routine disclosure must not be prohibited by the HIPAA privacy rules.
5. A request for a non-routine disclosure that is accompanied by an individual written authorization that is compliant with HIPAA will be honored in a manner consistent with the Plan's privacy policies. Pursuant to an individual's authorization, the information described in the authorization will be disclosed, even if that information is more than the minimum necessary information or additional information that is reasonably necessary to accomplish the purpose of the disclosure.

Requests

1. When requesting PHI from another health plan the Plan will make reasonable efforts to limit PHI to the minimum necessary information, or as determined by the Privacy Official, additional information that is the minimum necessary to accomplish the intended purpose.
2. When requesting medical records from a health care provider, the Plan will not request the entire medical file, but only that portion necessary to accomplish the intended purpose. If the Plan determines that the entire medical file must be requested, the Privacy Official must approve the request and authorization from the individual is required.
3. Plan staff will not request psychotherapy notes without written authorization from the individual. Psychotherapy notes are notes recorded in any medium by a health care provider who is a mental health professional documenting of analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. Psychotherapy notes are only those notes that are kept separate from the rest of the medical record. Summary medical information regarding psychotherapy may be used without written authorization if for treatment, payment or health care operations purposes.

Minimum necessary rule not applicable

Pursuant to the HIPAA privacy rules, the Minimum Necessary standard does not apply to the following uses, disclosures and requests for PHI:

1. Disclosures or requests to a health care provider for treatment purposes. The Plan does not generally engage in treatment, its services are limited to health care operations and payment. The treatment exception would generally only apply when information is requested by a health care provider for treatment purposes.
2. Disclosures to the individual who is the subject of the PHI. Identity of the individual must be verified.
3. Disclosures based on an authorization.
4. Disclosures to HHS for compliance and enforcement purposes related to HIPAA's administrative simplification requirements.
5. Uses or disclosures required by other laws.
6. Uses or disclosures required for compliance with HIPAA's electronic data interchange (EDI) transaction standards. Any required or situationally required EDI elements do not have to meet the minimum necessary test. However, the minimum necessary standard does apply to optional data elements.

3. Authorizations

Policy statement

This policy and procedure is adopted pursuant to Section 164.508 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by HHS, the Plan will follow the revised rules.

Except as otherwise provided under the privacy regulations or other applicable law, the Plan may not use or disclose PHI without a valid authorization. An authorization is not required for use or disclosure of PHI for treatment, payment or health care operations or for uses or disclosures otherwise permitted under the privacy rules.

If an authorization is asked for or received, the Plan will only use or disclose PHI in a manner consistent with the authorization.

Procedures

1. A valid authorization is required for any use or disclosure of PHI, except as provided under these procedures or under the privacy regulations.
2. An authorization is not required for use or disclosure of PHI for treatment, payment or health care operations.
3. The Plan will seek authorization for the following uses or disclosures of PHI, or when the Privacy Official determines an authorization is necessary:
    a. Use of health information to administer a claim for disability and/or pension benefits.
    b. Disclosure to a third party for purposes of assisting an employee to determine eligibility for benefits.
4. The Privacy Official will make a determination as to whether a specific use or disclosure of PHI requires an authorization.
5. The Plan will obtain an authorization for the use or disclosure of psychotherapy notes except:
    a. use or disclosure by the plan to defend a legal action, or
    b. use or disclosure to the Secretary of Health and Human Services (HHS) regarding compliance with HIPAA privacy rules,
    c. use or disclosure as required by law,
    d. use or disclosure for health oversight activities with respect to the oversight of the originator of the notes,
    e. use or disclosure to coroners and medical examiners,
    f. use or disclosures to an individual, when requested under, and as required by their right to inspect, copy and receive an accounting of their PHI, and
    g. use or disclosures, consistent with applicable law and standards of ethical conduct, where the Plan in good faith believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;

and is to a person reasonably able to prevent or lessen the threat, including the target of the threat.

6. The Plan will require authorizations for use or disclosure of PHI for marketing purposes or in the case of a sale of PHI. Refer to the Plan's Marketing and Prohibition on the Sale of PHI policy and procedure for more information.
7. Individuals always have the option to sign an authorization to disclose their PHI to the recipient(s) of their choice.
8. Authorizations will be used to disclose the PHI of a deceased individual for a period of 50 years following the individual's death. The authorization shall be executed by the personal representative of the deceased. After 50 years have passed, the individually identifiable information of the decedent will no longer be PHI, and as such, an authorization will no longer be needed to disclose that information.
9. When the form is completed and sent back by the covered individual, the Privacy Official will review the form to ensure that it is signed and complete. If the form has not been signed, is not properly completed or is otherwise defective, the Privacy Official will resend the form to the covered individual within ten business days with a specific explanation of the reason for rejecting the form.
10. The authorization must have an expiration date or event and must be signed and dated.
11. An authorization is not valid if:
    a. The expiration date has passed or the expiration event is known by the Privacy Official to have occurred.
    b. The authorization has not been filled out completely.
    c. The authorization is known by the Privacy Official to have been revoked.
    d. Any material information in the authorization is known by the Privacy Official to be false.
12. Authorizations should be on separate forms. If two authorizations are required, separate forms should be used.
13. The Plan will generally not condition the provision to an individual of treatment, payment, enrollment or eligibility on receipt of an authorization from the individual. However, the Plan may condition enrollment in the plan or eligibility for benefits on receipt of authorization prior to enrollment, if the authorization is sought for underwriting or risk rating determinations and does not relate to psychotherapy notes or genetic information.
14. If a personal representative signs the authorization form, then there must be proof of the representative's authority on file with the Privacy Official.
15. An individual may revoke an authorization at any time by providing a signed written notice to the Privacy Official by mail, facsimile or hand-delivery, or other method specified by the Privacy Official. An oral revocation will not be valid. A revocation will not be valid to the extent the Plan has relied on the authorization.
16. The Privacy Official will retain all authorizations for at least six years from the expiration date of the authorization, in accordance with the Plan's Record Retention policy and procedure.

4. Disclosure of protected health information (PHI) for public health, law enforcement, or legal process

Policy statement

This policy and procedure is adopted pursuant to Section 164.512 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If HHS changes the privacy rules, the Plan will follow the revised rules.

The Plan may use and disclose PHI for Public Health, Law Enforcement, or Legal Process purposes under the following conditions:

- The Plan may disclose this information without the consent or authorization of the individual who is the subject to the information.
- The Plan is not required to give the individual the opportunity to agree or object to the use or disclosure.
- These uses and disclosures must comply with the minimum necessary rule information that is minimally necessary to accomplish the business purpose. (Only uses and disclosures required by law are not subject to the minimum necessary rule.)
- In all cases involving these uses and disclosures, the Privacy Official or their designee must review and authorize the use or disclosure.
- Verification of the identity of public officials requesting PHI should be made pursuant to the Plan's Verification Policies and Procedures.
- The Plan will comply with the terms of this policy and procedure with respect to the PHI of living individuals, and of decedents for a period of 50 years following the date of the decedent's death. Fifty years after a decedent's death, his/her identifiable health information is no longer considered PHI protected by the privacy rule.
- The uses and disclosures listed below are permitted by the HIPAA privacy rules, but the Plan reserves the right to refuse to make the disclosure or to seek legal guidance regarding whether the disclosure should be made, including but not limited to seeking guidance from a court of applicable jurisdiction.

1. Uses and Disclosures Required by Law

   The Plan may use or disclose PHI to the extent that the use or disclosure is required by law. The use or disclosure must comply with and be limited to the relevant requirements of the law. If the use or disclosure is to report abusive situations, to comply with judicial or administrative legal process, or for law enforcement purposes, the use or disclosure must also comply with these policies and procedures.

   Uses and disclosures that are required by law are not subject to the minimum necessary rule.

   For example, the Plan may disclose PHI pursuant to an administrative subpoena, but the PHI must be limited to that authorized to be disclosed on the face of the subpoena.

2. Public Health

   The Plan may disclose PHI to public health authorities authorized by law to collect or receive PHI for the purpose of population-level activities to prevent disease in and promote the health of the population. This may include identifying, monitoring, preventing, or mitigating ongoing or prospective threats to the health or safety of a population, which may involve the collection of PHI.

   Public health does not include activities with any of the following purposes:

   a. To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating health care;
   b. to impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating health care; or
   c. to identify any person for any of the activities listed above.

   The Plan may disclose PHI at the direction of a public health authority to an official of a foreign government agency that is acting in collaboration with a public health authority.

3. Child Abuse or Neglect

   The Plan may disclose PHI to public health authorities or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

4. Food and Drug Enforcement Activity

   The Plan may disclose PHI to persons subject to the jurisdiction of the FDA for the purpose of activities related to the quality, safety or effectiveness of an FDA-regulated product or activity.

5. Communicable Disease

   The Plan will disclose PHI to a person who may have been exposed to a communicable disease, or may otherwise be at risk of contracting or spreading a disease or condition, if the Plan and the public health authority are authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

6. Safety Law Reporting and Employer Medical Surveillance

   The company may need PHI to comply with its obligations under state and federal law, including the Occupational Safety and Health Act (OSHA), the Federal Mine Safety and Health Act (FMSHA), and similar state laws that require the Plan to record illness or injury to carry out responsibilities for workplace medical surveillance.

   The Plan may, from time to time, employ or hire a covered health care provider to assist the Plan with these federal and state disclosure obligations, and for the following purposes:

   a. To conduct an evaluation relating to medical surveillance of the workplace or
   b. To evaluate whether the individual has a work-related illness or injury

   If the covered health care provider is a member of the Plan's workforce, he or she may, without authorization, disclose to the Fund in its capacity as employer PHI that consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance.

   In this case, the provider must give written notice to the individual that his or her PHI is disclosed to the Fund by either (1) giving the written notice to the individual at the time the

health care is provided or (2) if the health care is provided on the Fund's worksite, by posting the notice in a prominent place at the location where the health care is provided.

7. Victims of Abuse, Neglect, or Domestic Violence

   The Plan will disclose PHI about an individual whom the Plan reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence.

   Disclosure will be made only:

   a. After authorization by the individual;
   b. to the extent required by law and to the extent that the disclosure complies with the law;
   c. if expressly authorized by statute or regulation and the Plan believes, in the exercise of professional judgment, that the disclosure is necessary to prevent further harm to the victim or other people;
   d. if expressly authorized by statute or regulation and if a public official represents that an investigation will be adversely affected by waiting for authorization by the individual and that disclosure will not be used against the individual.

   The Plan must inform the individual of any disclosure unless the Plan believes informing the individual would place the individual at risk of serious harm, or if the Plan would be informing a personal representative who the Plan believes is responsible for the abuse or injury and informing the representative would not be in the best interests of the individual.

   This section does not apply to reports of child abuse or neglect, which are addressed in Section 3.

8. Health Oversight Activities

   The Plan will disclose PHI to a health oversight agency for oversight activities authorized by law, such as audits; investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for oversight of:

   a. The health care system;
   b. government benefit programs for which health information is relevant to beneficiary eligibility;
   c. entities subject to government regulation for which health information is necessary for determining compliance with program standards; or
   d. entities subject to civil rights laws for which health information is necessary for determining compliance.

   The Plan will not disclose PHI for an investigation or other activity in which the individual is the subject of the investigation and the investigation is not related to the receipt of health care, a claim for public benefits related to health, qualification for or receipt of public benefits or services when a patient's health is integral to the public benefits or services.

   Health oversight agencies include an agency or authority of the United States, including the Department of Labor, a State, a territory, a political subdivision of a state or territory, or an Indian tribe that is authorized by law to oversee the health care system (both public and private) or government programs described in this Section.

9. Disclosure in Response to a Court Order

   The Plan will disclose PHI in the course of any judicial or administrative proceeding in response to an order of a court or administrative tribunal. The Plan will disclose only the PHI expressly authorized by such order.

10. Disclosure in the Course of Judicial or Administrative Proceedings without a Court Order

    The Plan will not disclose PHI in response to a subpoena, discovery request or other lawful process unless the Plan verifies that the individual is aware of the request and has not made a valid objection to it, in accordance with the rules set forth in this Section.

    Counsel will be consulted when a subpoena, discovery request, or other lawful process is received.

    The Plan will disclose PHI in response to a subpoena, discovery request, or other lawful process, not accompanied by an order of a court or administrative tribunal, only if the Plan receives "written documentation" from the party seeking the PHI that: reasonable efforts have been made to ensure that the individual who is the subject of the PHI has been given notice of the request and either did not object or a court overruled the objection.

    Written documentation means a statement by the requestor that:

    a. The party requesting disclosure has made a good faith attempt to provide written notice to the individual whose PHI is being sought, or if the individual's location is unknown, has mailed a notice to the individual's last known address;
    b. the notice included sufficient information to allow the individual to go to court and object to the release; and
    c. the time for objections has expired or the court has resolved the objections.

    The Plan will also disclose PHI in response to a subpoena, discovery request, or other lawful process if the parties have agreed to a qualified protective order and have presented it to a court or administrative tribunal, or if the party seeking the PHI has requested a qualified protective order from such a court or administrative tribunal. A qualified protective order means an order of a court or administrative tribunal or a stipulation by the parties that prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which the PHI was requested. It must also require the return or destruction of the PHI (including all copies made) at the end of the proceeding.

11. Law Enforcement Purposes

    The Plan will disclose PHI for a law enforcement purpose to a law enforcement official. The Privacy Official will be responsible for this disclosure and must take reasonable steps to verify that an individual is a member of a law enforcement entity.

    The Plan is required by law to report certain types of wounds or other physical injuries.

    The Plan will disclose PHI as required by and as relevant to the following legal process:

    a. A court order, court-ordered warrant or subpoena, or summons issued by a judicial officer,
    b. a grand jury subpoena, or
    c. n administrative request, including an administrative subpoena or summons, or a civil or an authorized investigative demand, or similar process under law, **if** the PHI sought is relevant to a legitimate law enforcement inquiry, the request is specific and limited to

the purpose for which the information is sought, and certification is made that de-identified information could not be used.

The Plan will disclose PHI about an individual in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, but the Plan will supply only the following information:

a. Name and address;
b. Date and place of birth;
c. Social security number;
d. ABO blood type and Rh factor;
e. Type of injury;
f. Date and time of treatment;
g. Date and time of death, if applicable; and
h. 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.

The Plan will not disclose for the purposes of identification or location any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

12. PHI of Victims

The Plan will disclose PHI in response to a law enforcement official's request about an individual who is or is suspected to be a victim of a crime if:

a. The individual agrees to such disclosure, or
b. If the individual is unable to agree due to incapacity or other emergency circumstance, the law enforcement official must represent that PHI is needed to determine whether a violation of law by someone other than the victim has occurred, and that such information is not intended to be used against the victim, that immediate law enforcement activity which depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure, and that disclosure is in the best interests of the person.

The Plan will also disclose PHI about a deceased individual to law enforcement authorities if the Plan suspects the individual's death resulted from a criminal act. The Plan will disclose PHI if the Plan has a good faith belief that it is evidence of a crime on its premises.

13. Other Entities

The Plan will provide PHI to a coroner or medical examiner for the purpose of identification of a deceased person, determination of cause of death, or the coroner's other duties as authorized by law.

The Plan will also disclose PHI to funeral directors as necessary for fulfillment of their duties. If necessary, PHI may be disclosed prior to and in anticipation of the individual's death.

The Plan will disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.

14. Research

The Plan may provide PHI for research if a waiver is approved by an Institutional Review Board (IRB) or by an independent privacy board who has reviewed the effect on the individual's privacy rights. At least one board member must have no conflict of interest. The Plan must also receive representations from researchers that PHI will not be removed from its premises and that it is necessary for the research purposes.

Any such waiver must have an adequate plan to protect identifiers from disclosure and to destroy the identifiers at the earliest opportunity unless there is a justification for retaining the identifiers. They must also contain adequate written assurances that the PHI will not be reused or disclosed to any other person or entity.

The waiver must state that research could not practicably be conducted without access to and use of the PHI and must have a brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board. There must be a statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures.

15. Disclosure to Avert a Serious Threat to Health or Safety.

The Plan will disclose PHI if the Plan, in good faith, believes it to be necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Such disclosure must be to persons reasonably able to prevent or lessen the threat, including the target of the threat. The Plan will also disclose if the Plan believes in good faith that it will be necessary for law enforcement to identify or apprehend an individual the Plan believes may have caused serious physical harm to the victim because of a statement by an individual admitting participation in a violent crime. Such information must be limited to:

a. Name and address;
b. Date and place of birth;
c. Social security number;
d. ABO blood type and Rh factor;
e. Type of injury;
f. Date and time of treatment;
g. Date and time of death, if applicable; and
h. 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.

If a workforce member who is the victim of a criminal act discloses PHI to a law enforcement official provided that 1) the PHI disclosed is about the suspected perpetrator of the criminal act and 2) the PHI is limited to the information to the bulleted list above.

The Plan will not disclose for the purposes of identification or location any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

The Plan may also disclose PHI when it is necessary for law enforcement to identify or apprehend an individual who is believed to have escaped from a correctional institution or lawful custody.

The Plan may not disclose PHI relating to an individual's therapy or request for therapy to treat a propensity to commit the criminal conduct that is the basis for the disclosure.

16. National Security

    The Plan will disclose to the U.S. Armed Forces PHI of individuals serving in the armed forces when deemed necessary by military authorities to assure execution of the military mission, if the military authority has published in the Federal Register the following information:

    a. Appropriate military command authorities; and
    b. the purposes for which the PHI may be used or disclosed.

    The Plan will disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333). The Plan will also disclose PHI to officials for the protection of the President or other persons or to foreign heads of state.

17. Inmates

    The Plan will disclose PHI to Correctional Institutions and other law enforcement custodial situations if law enforcement represents that PHI is necessary for the provision of health care to the individual. The Plan will also disclose if necessary for the health and safety of the individual or others at the correctional institution or other persons responsible for the transportation of inmates and maintenance of safety, security, and order of the correctional institution. An individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

18. Health Plans

    A health plan that is a state or local government program providing public benefits may disclose PHI relating to eligibility or enrollment in the health plan to another government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies is authorized by statute, is necessary to coordinate the covered functions of such programs, or is necessary to improve management of such programs.

19. Workers' Compensation

    The Plan may disclose PHI as authorized and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault. Workers' compensation disclosures that are required by law are not subject to the minimum necessary rule.

20. Disclosures by Whistleblowers

    If a workforce member believes in good faith that the Plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, the workforce member may disclose PHI to 1) a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity; or 2) by an attorney retained by or on behalf of the workforce member for the purpose of determining the legal options of the workforce member with regard to the conduct of the Plan.

21. Compliance with HIPAA

    The Plan must permit HHS access during normal business hours to its facilities and information, including PHI, that is pertinent to ascertaining compliance with the applicable requirements of HIPAA. If HHS determines that exigent circumstances exist, such as the destruction of documents, the Plan must permit access at any time without notice. Disclosures made to HHS in accordance with a HIPAA compliance investigation are not subject to the minimum necessary rule. See *Section 164.502(b)(2)(iv)*.

    If any information required of the Plan under this section is in the exclusive possession of any other agency or person and the other agency or person fails or refuses to furnish the information, the Plan must set forth what efforts have been made to obtain the information.

Procedures

1. Disclosures of PHI without the authorization of the individual may be made in accordance with the Plan's policies.
2. A request to inspect and/or copy PHI must be made in the manner prescribed by the Plan.
3. Requests from Public Officials shall be verified using the Plan's Verification Policy and Procedures for requests from Public Officials.
4. The Plan may charge the following fees:
    a. Costs of creating or copying PHI including labor and supplies (for electronic or hardcopy information),
    b. postage for mailing the PHI, and
    c. the cost of preparing a summary of PHI.
5. The Plan will maintain records of the request for disclosure, date of disclosure, requesting party's name and address, reason for the disclosure, and a copy of the subpoena, court order, or other applicable documents.

5. Certification & Plan Document Amendment

Policy statement

This policy and procedure is adopted pursuant to Section 164.504(f) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If HHS changes the privacy rules, the Plan will follow the revised rules.

Group health plans can disclose PHI to plan sponsors if plan sponsors voluntarily agree to use and disclose the information only as permitted or required by the regulation. The information may be used only for Plan administration functions performed on behalf of the Plan which are specified in the Plan's documents. Plan administration functions include quality assurance, claims processing, auditing, monitoring, and management of carve-out plans such as vision and dental. It does not include any employment-related functions or functions in connection with any other benefits or benefit plans, and group health plans may not disclose information for such purposes absent an authorization from the individual.

Insured benefit programs

For its insured benefit programs, if subject to the privacy rules as referenced herein, the Board of Trustees will certify to a health insurance issuer, HMO, or Group Health Plan that the Board of Trustees is in compliance with the Privacy Rules. The certification will allow the health insurance issuer, HMO, or Group Health Plan to disclose individually identifiable health information to the Board of Trustees for plan administration functions only. Generally, the issuer or HMO will have a certification form for the Board of Trustees to sign, which should be reviewed by Legal Counsel.

Self-insured benefit programs

The Plan Sponsor must amend its Plan Documents to include provisions that permit the Plan to share PHI with the Plan Sponsor. These Plan Document amendments must:

1. Describe the permitted uses and disclosures of PHI;
2. Specify that disclosure is permitted only upon receipt of a certification from the Plan Sponsor that the plan documents have been amended and the Plan Sponsor has agreed to certain conditions regarding the use and disclosure of PHI; and
3. Provide adequate separation between plan administration activities and all other activities such as to:
    a. Identify the employees or classes of employees who will have access to PHI;
    b. Restrict access solely to the employees identified and only for the functions performed on behalf of the Plan; and
    c. Provide a mechanism for resolving issues of noncompliance.

4. Additionally, the Plan Sponsor must certify to the Plan that the Plan Sponsor agrees to:
    a. Not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
    b. Ensure that any subcontractors or agents to whom the Plan Sponsor provides PHI agree to the same restrictions;
    c. Not use or disclose the PHI for employment-related actions or for use by other employee benefit plans;
    d. Report to the Plan any use or disclosure that is inconsistent with the plan documents or this regulation;
    e. Make the PHI accessible to individuals as required under these policies;
    f. Allow individuals to amend their information;
    g. Provide an accounting of its disclosures;
    h. Make its practices available to the Secretary of HHS for determining compliance;
    i. Return and destroy all PHI when no longer needed, if feasible; and
    j. Ensure that adequate separate exists between plan administration activities and all other activities.

6. Business associates

Policy statement

This policy and procedure is adopted pursuant to Sections 164.502(e), 164.504(e), 164.532(d) and (e)of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the privacy rules are changed by HHS, the Plan will follow the revised rules.

The Privacy Rule allows health plans to disclose PHI to these business associates if the plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. Covered entities, such as the Plan, may disclose PHI to an entity in its role as a business associate only to help the Plan carry out its health care functions — not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

The Plan will obtain satisfactory assurance from its business associates that the business associate will appropriately safeguard the PHI it receives or creates on behalf of the Plan. The satisfactory assurance must be in writing in the form of a contract or business associate agreement.

Procedures

The Plan will assure that a business associate agreement is in writing for each Plan business associate.

7. De-identification

Policy statement

This policy and procedure is adopted pursuant to Section 164.514 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule dated November 26, 2012. If the privacy rules are changed by HHS, the Plan will follow the revised rules.

The Plan may disclose health information that has been "de-identified" without observing other HIPAA-required policies and procedures, because de-identified information is not subject to the HIPAA privacy rules.

Health information that does not identify an individual, that complies with the de-identification policies and procedures, and which the Plan believes cannot be used to identify an individual is considered "de-identified."

If reasonable, to the extent possible, the Plan will use de-identified information for plan administration purposes.

Procedures

The following information is de-identified information:

1. Information is de-identified when a person with knowledge of generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information disclosed could be used, alone or in combination with other reasonably available information, to identify an individual who is a subject of the information. The Plan must receive documentation of the methods and the result of the analysis that justify this determination. If this procedure is used, the expert will comply with the guidance set forth in the Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule dated November 26, 2012; or
2. The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed, and the Plan does not have knowledge that the information provided could be used alone or in combination with other information to identify an individual who is a subject of the information:
    a. Names;
    b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip codes. The initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people. If the geographic units which make up the initial three digits of a zip code contain 20,000 or fewer people, the first three digits must be changed to 000. Utilizing Census 2000 data, zip codes with the following initial three digits must have the zip code changed to 000: If more current data has been published that data should

be utilized. 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, 893.

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;

   1) For example, de-identified information could not include the date and month of a medical procedure or event (i.e., 1/1/2009), but it may include only the year (i.e., 2009).

   2) Age may be included in de-identified information, except that ages over 89 must be indicated as 90 or above, whether the actual age is stated or implied (i.e., if the birth year is 1910 and treatment is provided in 2010, the birth year must be reported as “on or before 1920”).

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;

r. Any other unique identifying number, characteristic, or code, except as permitted for re-identification of the data as set forth below; and

s. Parts or derivatives of any of the above-listed identifiers may not be included in de-identified information. For example, de-identified information may not include the last four digits of an individual’s social security number or participants’ initials.

3. Reidentification

The Plan may assign a code or other means of record identification to allow de-identified information to be re-identified by the Plan, provided that:

a. Derivation. 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 to identify the individual; and

b. Security. The Plan does not use or disclose the code or other means of record identification for any other purpose, and do not disclose the mechanism for re-identification.

8. Verification

Policy statement

This policy and procedure is adopted pursuant to Section 164.514(h) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the privacy rules are changed by HHS, the Plan will follow the revised rules.

1. General Policy: It is the policy of the Plan to verify the identity of an individual or entity requesting PHI, and to verify the authority of such individual to have access to PHI, before the PHI is disclosed to the individual, if the identity or any such authority of the individual is not known to the Plan.

   It is also the policy of the Plan to obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement or representation is a condition of the disclosure under HIPAA. The Plan may rely, if such reliance is reasonable under the circumstances, on documentation, statements or representations that, on their face, meet HIPAA's requirements.

2. Public Officials: Administrative Requests from Law Enforcement Officials: If the conditions required before the Plan can disclose information to a law enforcement official pursuant to an administrative request are met, then the verification requirements are satisfied by the administrative subpoena or similar process, or by a separate written statement that, on its face demonstrates that the applicable requirements have been met. No additional verification is required. See *Law Enforcement Policy and Privacy regulation section 164.512(f)(1)(ii)(C)*.

   Identity and Authority of Other Public Officials: The identity and authority of all other public officials must be verified in the manner set out in the Plan's Verification Procedure for Public Officials.

3. Imminent Serious Threat to Health and Safety: A disclosure to an individual or entity pursuant to section 164.512(j)(1)(i) (other than to a public official) to avert an imminent threat to health or safety is allowed without further verification if the Plan has a good faith belief that the disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public, and the disclosure is to a person reasonably able to prevent or lessen the threat. If these conditions are met no further verification is needed. In such emergencies the Plan is not required to demand written proof that the person requesting the PHI is legally authorized. The Plan can reasonably rely on verbal representations.

4. Where Verification is Not Required: This policy does not apply to disclosures made under section 164.510 of HIPAA's privacy regulation regarding disclosures for facility directories, and disclosures for involvement in an individual's care and for notification purposes. Verification is not required for these disclosures.

Procedures

1. When Required:

   Subject to any exceptions noted in the Plan's verification policy, unless an individual or entity is requesting PHI in person and the identity and authority of the individual or entity is

personally known to Plan Office representatives, the Plan must verify the identity and authority of the individual. Individuals are deemed to have the authority to obtain their own PHI, unless otherwise indicated.

2. Manner of Verifying Identity:
    a. Request in Person for Individual's Own PHI: If an individual makes a request for their own PHI in person, they must show the Plan at least one piece of identification such as a driver's license, passport or union card to verify their identity.
    b. Request by Telephone or Electronically for Individual's Own PHI: Plan staff responding to a request by telephone for an individual's own PHI must verify the individual's identity by asking them to verify factual information in their file, based on procedures developed by the Plan.
    c. Request by Mail or Fax for Individual's Own PHI: Any request for disclosure of PHI by mail or fax must be accompanied by a copy of at least one form of identification such as a driver's license, passport or union card to verify their identity. Documents must be mailed to the last-recorded mailing address of the individual, unless a written change of address form has been received.
    d. Requests on Behalf of Another: PHI will not be disclosed to an individual requesting this information on behalf of another, unless the individual is a personal representative of the individual (as set out in the Plan's Personal Representative Policy). Plan staff will confirm the authority of a person to act on behalf of the individual by making sure that the personal representative procedure has been followed (i.e., a personal representative designation has been completed indicating the authority of the individual to act on behalf of another). The individual acting on behalf of another must show their identity by providing at least one piece of identification such as a driver's license, passport or union card to verify their identity. Spouses and parents/guardians must also verify their relationship to the individual, in addition to verifying their identity, by providing a copy of a minor's birth certificate, social security card, etc.
    e. Requests involving a translator: If an individual requests that a translator assist them in discussing PHI with the Plan's staff the Plan shall either obtain an authorization (and verify identity of the translator) or follow the procedure set forth in the Plan's policy for Involvement in an Individual's Care.
    f. Requests by Health Care Providers: PHI will be disclosed to a Health Care Provider for purposes related to the payment or health care operations of the Plan. If the Health Care Provider calls via telephone, the Plan will disclose PHI after it verifies the identity of the Provider.
    g. Requests by Public Officials:
        1) Identifying Public Official — The Plan will rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity of a public official or a person acting on behalf of a public official:
            a) If the request is made in person, presentation of an agency identification badge, other official credential, or other proof of government status;
            b) If the request is in writing, the request is on appropriate 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, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

2) Confirming Authority of Public Official — The Plan will rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official (this confirmation cannot be completed via telephone):
    a) A written statement of the legal authority under which the PHI is requested, or if a written statement is impractical, an oral statement of such legal authority;
    b) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal is presumed to constitute legal authority.

h. Requests by Other Parties: When an entity (other than the individual themselves, a personal representative, or public official) requests disclosure of PHI that is otherwise allowed under HIPAA and the Plan's Policies and Procedures, their identity and authority must also be confirmed. An entity will have the authority to receive the information only if a valid authorization is completed pursuant to the Plan's authorization policy.

9. Recognition of personal representative

Policy statement

This policy and procedure is adopted pursuant to Section 164.502 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and pursuant to section 2560.503-1 of the claims and appeals regulation under the Employee Retirement Income Security Act ("ERISA"). If the privacy rules are changed by HHS, the Plan will follow the revised rules.

1. The Plan will treat a personal representative as the individual for purposes of implementing the HIPAA privacy rules and ERISA's claims and appeals procedure rules.
    a. The personal representative may only have access to PHI that is consistent with and relevant to the scope of authority set out in the personal representative form.
    b. The Plan may elect not to treat a person as the personal representative of an individual if:
    c. The Plan Administrator or the Privacy Official has a reasonable belief that:
        1) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
        2) Treating such person as the personal representative could endanger the individual; and
        3) The Plan Administrator or the Privacy Official, in the exercise of professional judgment, decide that it is not in the best interest of the individual to treat the person as the individual's personal representative.
2. **Dependents (Other Than Spouses) Including Unemancipated Minors:** The Plan will consider a parent, guardian or other person acting in loco parentis as the personal representative of an unemancipated minor unless applicable law requires otherwise, or the Plan agrees to abide by a participant or beneficiary request that the Plan restrict disclosure of PHI to a parent, guardian or other person acting in loco parentis.
    a. A parent, guardian or other person acting in loco parentis of a minor will not be treated as a personal representative (and the minor has the authority to act as an individual), with respect to PHI pertaining to a health care service, if:
        1) The minor consented to such health care service
        2) The minor, a court or another person authorized by law consented to such health care services; or
        3) A parent, guardian, or other person acting in loco parentis assented to an agreement of confidentiality between a covered health care provider and the minor with respect to the services.

    If a parent, guardian, or other person acting in loco parentis is not treated as a minor child's personal representative for a particular service, the parent, guardian, or other person acting in loco parentis may be permitted access to a minor's PHI under the individual right to inspect and copy PHI if the decision to provide access is made by a licensed health care professional in the exercise of his or her professional judgment, and the decision is consistent with state law.

3. **Deceased Individuals**: The Plan will automatically recognize the following persons as personal representatives of deceased individuals or their estates:
    a. Executors
    b. Administrators
    c. Other persons with authority to act on behalf of the deceased individual or their estate.

    The Plan will comply with the terms of this policy and procedure with respect to the PHI of a decedent for a period of 50 years following the date of such decedent's death. After 50 years have passed, the individually identifiable health information of the decedent is no longer considered PHI protected by the privacy rules.
4. **Treating Physician Regarding an Urgent Claim**: In the case of an "urgent claim," a "health care professional" (as these terms are defined in ERISA's claims regulation) with knowledge of a participant or beneficiaries medical condition will be automatically recognized by the Plan as a personal representative. The health care professional is deemed to be a personal representative only with respect to the disclosure of PHI directly relating to the urgent claim.
5. **Power of Attorney**: The Plan will automatically recognize any person who holds a legal power of attorney for an individual as that individual's personal representative.
6. **Other Applicable Law**: The Plan will recognize any person who is authorized under State or other applicable law (e.g., court-appointed legal guardian) to act on behalf of the individual in making health care related decisions as that individual's personal representative.
7. The Plan may disclose PHI to an individual who is not a personal representative (or deemed to be a personal representative) if they are a family member, other relative or close personal friend of the individual, or any other person identified by the individual, and the disclosure is directly relevant to such person's involvement with the individual's care or payment for the individual's care pursuant to sections 164.510(b) of HIPAA's privacy regulation. This rule extends to the PHI of a decedent, unless doing so is inconsistent with any prior expressed preference of the decedent that is known to the Plan. See *the Plan's Policy and Procedure for Uses and Disclosures for Involvement in an Individual's Care and for Notification Purposes*.
8. Where a personal representative form has been completed and approved, it will be recognized by the Plan if the individual making the designation is covered by the Plan. The individual has a right to revoke the designation at any time by submitting a signed statement to the Plan revoking the designation. To designate another individual as personal representative, a new personal representative form must be completed and approved by the Plan.

Procedures

Other than those individuals deemed to be personal representatives in paragraph 2 of the Policies related hereto, the Plan will only treat an individual as a personal representative where a personal representative form has been filled out that meets standards established by the Plan Sponsor, and the Plan office has approved the designation. Individuals may request a copy of the personal representative form by calling the Plan. All personal representatives will be subject to the Plan's verification procedure.

10. Use & disclosure for involvement in an individual's care and for notification purposes

Policy statement

This policy and procedure is adopted pursuant to Section 164.510(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by HHS, the Plan will follow the revised rules.

The Plan may disclose to a family member, other relative, or a close friend of an individual, or to any other person identified by the individual, PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. This disclosure can only be made where the individual that is the subject of the PHI is given the opportunity to agree or object according to the Plan's Procedure for Use & Disclosure for Involvement in an Individual's Care and for Notification Purposes.

The Plan may also use and 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. Any such use or disclosure must be made according to the Plan's Procedure for Use & Disclosure for Involvement in an Individual's Care and for Notification Purposes.

In addition, the Plan may disclose a decedent's PHI to a family member, other relative, or close personal friend of the decedent, or any other person previously identified by the decedent to the Plan if the disclosure is directly relevant to such person's involvement with the decedent's care or payment related to the decedent's health care, unless doing so is inconsistent with any prior expressed preference of the decedent that is known to the Plan. The Plan will comply with the terms of this policy and procedure with respect to the PHI of a decedent for a period of 50 years following the date of such decedent's death. After 50 years have passed, the individually identifiable health information of the decedent is no longer considered PHI protected by the privacy rules.

The general purpose of this rule is to allow disclosure in those limited instances where disclosure of protected information to next-of-kin (or to those with a close relationship to an individual) is necessary, or it is needed to locate next-of-kin or other individuals involved in their care. This policy will also allow disclosure of PHI to disaster relief organizations under certain circumstances.

Disclosures made under this policy and procedure are not subject to the Plan's verification policy.

Exceptions:

1. This policy and procedure will not apply to disclosures to individuals who are personal representatives in accordance with the Plan's Recognition of Personal Representative Policy & Procedure.
2. This policy and procedure does not apply to disclosures made to avert an imminent threat to health or safety, as described in section 11 of the Plan's Policy Regarding the Disclosure for Public Health, Law Enforcement, or Legal Process.

Procedures

The following procedures must be followed before PHI is disclosed to a person involved in an individual's care or for notification purposes:

1. Use or Disclosure with the Individual Present. If an individual is present for, or otherwise available prior to a use or disclosure to those involved in an individual's care or for notification purposes, and the individual has the capacity to make health care decisions, the Plan may use or disclose PHI if the Plan:
    a. Obtains the individual's agreement (either orally or in writing)
    b. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
    c. Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

    This procedure may be followed when a translator accompanies an individual.
2. Limited Uses and Disclosures When the Individual is not Present. If an individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the Plan may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care. The Plan may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interests in allowing a person to act on behalf of the individual in obtaining PHI on their behalf to assist an individual in their care or payment for their care.
3. Use and Disclosure for Disaster Relief Purposes. The Plan may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted to notify or assist in notifying persons involved in an individual's care. Disclosures to these entities must be made according to section 1 and 2 above where the Plan determines, in the exercise of its professional judgment, that the requirements in section 1 and 2 do not interfere with the ability to respond to an emergency situation.
4. Documentation. All written agreements to allow disclosure or written objections to the disclosure must be kept according to the Plan's Record Retention policy.

11. Claims and appeals

Policy statement

This policy and procedure is adopted pursuant to Section 164.502 (g) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, the Plan will follow the revised rules.

The Plan will safeguard the privacy of PHI used and disclosed during the claims and appeal process by using and disclosing only the information that is minimally necessary to make claims determinations and appeals, and by limiting access to PHI to only those Plan staff and service providers (Business Associates) that need to review this information. (See *Minimum Necessary Policy*.) In addition, in dealing with PHI involving health claims, the Plan will recognize all individuals' rights required by HIPAA and set forth in the Plan's Individual Rights Policies and Procedures.

Procedures

The Plan, at a minimum, will incorporate the following procedures within the claims process:

1. Initial Claim Review
    a. Access to health information used and disclosed for an initial determination on a claim will be limited to those individuals who process health claims. The positions of those allowed to have access to claims PHI will be documented and access controls implemented.
    b. PHI provided to Business Associates and/or insurers who perform services for the Plan in administering and insuring benefits will be limited to only that which is minimally necessary.
    c. All claims logs and other information kept to ensure consistent claims decision making shall be safeguarded under the Plan's Administrative, Technical, and Physical Safeguards Policy and Procedure.
2. Appeals
    a. Information compiled for the appeals will exclude the following information unless necessary: name, social security number, dependent name, employer, address, and telephone number. Only documents relevant to the claim will be provided to the reviewer.
    b. When a specific claim is reviewed during an appeals meeting, only those individuals involved in making the determination (or assisting in making a determination) shall be present. All others must exit the room.
    c. Any PHI provided to the appeals committee during the meeting will be returned to the Plan after the meeting.
    d. Efforts will be made to safeguard PHI contained in Meeting minutes. For example, meeting minutes will be kept according to the Plan's Administrative, Technical, and Physical Safeguards Policy. Information will be redacted from the meeting minutes where necessary.

e. The notice of appeal determination will only be sent to the individual making the appeal request (subject to the Plan's rules regarding personal representatives, person's involved in an individual's care/payment, or other individual where authorization is not required under the HIPAA privacy rules).

3. Individual Inquiries on Claims. All inquiries concerning claims that involve the disclosure of PHI are subject to the Plan's Policy and Procedure to verify the identity and authority of the individual making the request. In addition, any Plan disclosure of PHI in response to inquiries made on behalf of another will only be made with an individual authorization, unless the individual requesting the PHI is a personal representative, someone involved in an individual's care/payment, or other individual where authorization is not required under the HIPAA privacy rules. All PHI concerning claims obtained in responding to individual inquiries will be safeguarded pursuant to the Plan's Security and Record Retention Policy and Procedure.

12. Distribution of privacy notice

Policy statement

This policy and procedure is adopted pursuant to Section 164.520 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

The Plan will prepare and distribute a Privacy Notice describing the Plan's privacy policies and procedures. The Notice will be provided to covered individuals at the following times:

1. Upon request;
2. no later than April 14, 2003 to plan participants (i.e., individuals that are participants as of the date the notice is mailed);
3. to all new enrollees at the time of enrollment; and
4. within 60 days of a material revision in the Privacy Notice.

Procedures

1. The Privacy Official (or the Privacy Official's designee) will ensure that the Privacy Notice is provided to new participants as part of the enrollment materials or in connection with the new participant counseling process (unless a Privacy Notice was provided to that individual within the past 12 months).
2. Once every three years, the Privacy Official (or the Privacy Official's designee) will notify participants that the Privacy Notice is available.
3. Whenever there is a material revision to the Privacy Notice, a copy will be mailed by the Privacy Official (or the Privacy Official's designee) to participants within 60 days of the revision.
4. The Privacy Official (or the Privacy Official's designee) will ensure that the Privacy Notice is prominently posted and available on the Plan website.
5. The Plan may send the Privacy Notice by email to any covered individual who agrees to electronic notice. However, the Plan will still provide a paper copy of the Privacy Notice upon request or if the Plan knows that the email was not received.
6. The Privacy Official (or the Privacy Official's designee) will maintain a copy of the initial Privacy Notice, as well as any revised versions of the Notice, in accordance with the Plan's Record Retention Policy.

13. Training

Policy statement

This policy and procedure is adopted pursuant to Section 164.530(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

It is the policy of the Plan to train the Plan's workforce, including all Plan personnel, on all Plan policies and procedures concerning the use or disclosure of PHI implemented for compliance with the privacy requirements under HIPAA, and the breach notification requirements under the Health Information Technology for Economic and Clinical Health Act (HITECH)

Procedures

1. The Plan shall keep records of training and attendance.
2. The Plan shall identify the roles that use or disclose PHI and the appropriate training necessary for each role.
3. All individuals in the Plan's workforce shall be trained on a periodic basis.
4. New employees of the Plan will be trained within a reasonable time after they become employed by the Plan.
5. Training will also be provided to each member of the Plan staff whose functions are affected by a material change in the Plan's policies and procedures. This training will take place within a reasonable time after the material change in policy or procedure becomes effective.
6. The Plan will re-train Plan personnel as necessary.
7. The Plan will train temporary employees and independent contractors as necessary based on their assignment.

14. Complaints for violation of HIPAA privacy rules

Policy statement

This policy and procedure is adopted pursuant to Section 164.530(d) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

The Plan accepts and will investigate complaints of violations of the Plan's privacy policies and procedures from covered individuals, including complaints regarding the Plan's compliance with the breach notification rule, as well as complaints from Plan staff.

The Privacy Official (or the Privacy Official's designee) will determine:

1. Whether there has been a violation of the Plan's privacy policies and procedures;
2. The seriousness and effect of the violation; and
3. Any corrective action that may be taken.

The Privacy Official (or the Privacy Official's designee) will document all complaints received and their outcomes, if any.

Procedures

Form of Complaints

1. Complaints must be in writing. They may be on the Plan's Complaint Form or they may be in another written form. Complaints must contain:
    a. The date of the complaint;
    b. The date of the alleged violation or other action that is the subject of the complaint;
    c. The name or position of the party against whom the complaint is made;
    d. The substance of the complaint; and
    e. The name and signature of the complainant.
2. The Plan will accept written complaints from covered individuals and from Plan employees. When Plan employees receive oral complaints from covered individuals, they will inform individuals that complaints must be in writing and will send the individuals complaint forms to complete and return to the Plan. Plan employees may submit complaints orally or in writing.
3. The Plan staff will date-stamp the complaint when it is received.
4. The Plan staff will forward written complaints to the Privacy Official (or the Privacy Official's designee) for review.

Disposition of Complaint

1. The Privacy Official (or the Privacy Official's designee) will:
    a. Investigate the complaint;
    b. Question the covered individual or employee making the complaint, if necessary;

c. Question the party alleged to have violated the privacy policies and procedures;
d. Consider any documents, evidence, or testimony offered on behalf of the party alleged to have violated the plan's privacy policies and procedures;
e. Determine whether there has been a violation of the plan's privacy policies and procedures;
f. Determine whether any corrective action is necessary as a result of the complaint;
g. Implement any corrective measures necessary as a result of the complaint;
h. Document any corrective measures taken;
i. When appropriate, inform the employee, participant, or beneficiary of the determinations made with regard to the complaint;
j. Make and keep a record of the complaint investigation, including the complaint and the plan's findings, to ensure consistency of determinations and corrective measures for similar violations; and
k. Retain written records for six years beginning from the date on which there is a disposition of the complaint.

2. The Privacy Official (or the Privacy Official's designee) will make a disposition of the complaint within 60 days of the date that the complaint is date stamped in the Plan.
3. The Plan will not require individuals to waive their right to complain to the Secretary of HHS about the Plan or business associate not complying with the privacy rule or the breach notification rule under the HITECH Act as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

15. Anti-retaliation

Policy statement

This policy and procedure is adopted pursuant to Section 164.530(g) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

In compliance with Section 164.530, the Plan will not take retaliatory action against any person who files a complaint with the Plan or with the Department of Health and Human Services.

The Plan will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any individual for exercising his or her rights under the HIPAA privacy rules or breach notification rules under the HITECH Act or for filing a complaint or participating in other process established by the HIPAA privacy rules; or
2. Any individual or other person or entity for filing a complaint about our HIPAA privacy compliance with the secretary of health and human services; or
3. Any individual or other person or entity for testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or
4. Any individual or other person or entity for opposing any act or practice made unlawful by HIPAA or the HITECH Act, provided the individual or person or entity has a good faith belief that the practice opposed is unlawful. The manner of the opposition must be reasonable and not involve a disclosure of PHI in violation of HIPAA privacy rules or breach notification rules of the HITECH Act. For example, an employee who discloses PHI to the media or friends is not protected.

16. Mitigation of harmful effects

Policy statement

This policy and procedure is adopted pursuant to Section 164.530(f) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

In compliance with Section 164.530, Plan will mitigate, to the extent practicable, any harmful effects known to us by a use or disclosure of PHI in violation of our policies and procedures or HIPAA privacy rules by employees of the Plan or any Business Associate.

In order to mitigate harmful effects, the use or disclosure of PHI that violates our procedures and/or HIPAA must be known to us. This means the Privacy Official (or the Privacy Official's designee) must have been informed of the violation by an individual, a member of the Plan's workforce, or a Business Associate.

When mitigating harmful effects, the Plan will take reasonable steps based on knowledge of where the information has been disclosed, how it might be used to cause harm to an individual, and what steps can actually have a mitigating effect in that specific situation.

17. Sanctions for violation of HIPAA privacy rules

Policy statement

This policy and procedure is adopted pursuant to Section 164.530(e) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

An employee of the Plan who is responsible for handling PHI of covered individuals will be sanctioned for violating the HIPAA privacy rules, the breach notification rules under the HITECH Act, and the privacy policies and procedures adopted by the Plan.

The Privacy Official (or the Privacy Official's designee) will determine whether there has been a violation of the HIPAA privacy rules, the seriousness and effect of the violation, and the sanction to be imposed on the employee.

The Privacy Official (or the Privacy Official's designee) has discretion to determine appropriate sanctions for violation of the HIPAA privacy rules. Sanctions will include disciplinary action up to and including dismissal.

Procedures

Determination of violation

1. All Plan employees are required to report any perceived violations of the HIPAA privacy rules to the Privacy Official. Reports may be made orally or in writing.
2. The Privacy Official (or the Privacy Official's designee) will:
    a. Investigate the alleged violation of the HIPAA privacy rules;
    b. Question the employee reporting the perceived violation;
    c. Question the employee who is alleged to have violated the HIPAA privacy rules;
    d. Consider any evidence or testimony accompanying the report of violation or submitted on behalf of the employee alleged to have violated the HIPAA privacy rules;
    e. Determine whether there has been a violation of the HIPAA privacy rules; and
    f. Make and keep a record of the investigation.

Determination of sanction

1. The Privacy Official (or the Privacy Official's designee) will determine:
    a. The gravity of the violation of the HIPAA privacy rules; and
    b. The appropriate sanction to be imposed on the employee.
2. The Privacy Official (or the Privacy Official's designee) has discretion to determine appropriate sanctions and will consider:
    a. Whether the violation is accidental or egregious; and
    b. Whether it is a first-time violation or a repeated violation.

3. The Privacy Official (or the Privacy Official's designee) will make and keep a record of sanctions imposed to ensure consistency of sanctions for similar violations.
4. Sanctions will not be imposed for disclosures of PHI that meet the conditions set out in sections 164.530(g)(2) and 164.502(j) of the HIPAA privacy rules regarding whistleblower protections.

18. Marketing

Policy statement

This policy and procedure is adopted pursuant to the sections 164.501 and 164.508(a)(3) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

Marketing

Subject to the definitions and exceptions below, the Plan will obtain an authorization to disclose PHI to market products and services to participants and beneficiaries, unless the marketing is in the form of:

- A face-to-face communication by the entity with the individual whose PHI is being disclosed,
- A promotional gift of nominal value to the individual whose PHI is being disclosed,
- Communications that generally promote good health, or
- Information regarding government programs.

If the marketing involves direct or indirect remuneration to the Plan from a third party, the authorization will state that such remuneration is involved.

“Marketing” for the purposes of this policy shall mean to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing includes an arrangement between the Plan and any other entity whereby the Plan discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

The following activities are not marketing, and therefore can be done without the Plan obtaining an individual authorization:

- A communication to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the Plan in exchange for making the communication is reasonably related to the Plan’s cost of making the communication. In addition to refill reminders, these communications may include information about generic equivalents, medication adherence or how to take a biologic or self-administered medication.
- A communication describing a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Plan, including communications about the entities participating in the Plan’s network, replacement of, or enhancements to, the Plan, and health-related products or services available only to a participant that add value to, but are not part of, a plan of benefits;
- A communication made for treatment of the individual by a health care provider; and
- A communication for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, providers, or settings of care to the individual.

Prohibition on sale of PHI

Subject to the exceptions below, the Plan will obtain an authorization to disclose PHI if it is receiving direct or indirect remuneration from or on behalf of the recipient of the information in exchange for the information.

- For this purpose, “sale of PHI” includes transactions that involve a transfer of ownership of PHI, as well as exchanges of PHI under access, license or lease agreements, and any other exchanges of PHI for which remuneration is made.
- Remuneration includes financial payments or non-financial benefits (such as, benefits in kind). Direct remuneration is that which is received directly from the recipient of the PHI, and indirect remuneration is that which is received on behalf of the recipient of the PHI from another entity.

The following disclosures are excepted from the prohibition on the sale of PHI, and therefore, no authorization is required to make these disclosures, even if the Plan receives remuneration:

- Disclosures for public health purposes under 164.512(b) or 164.514(e);
- For research purposes pursuant to 164.512(i) or 164.514(e) as long as remuneration is subject to certain limitations;
- For treatment and payment purposes;
- For the sale, transfer, merger or consolidation of all or part of the plan and for related due diligence;
- To a business associate for activities that the business associate undertakes on behalf of the Plan, and the only remuneration is for the performance of the business associate activities on behalf of the Plan;
- To an individual who makes a request for access (*see Policy on Right of Access to PHI*) or a request for an accounting of disclosure (see *Policy on Right to Accounting of Disclosures of PHI*);
- As required by law as permitted under 164.512(a); and
- For any other purpose permitted by these Policies and Procedures and the privacy rule, as long as any remuneration is limited to a reasonable, cost-based fee to cover the cost to prepare and transmit the PH for that purpose, or a fee that is permissible by other law.

Procedure

The Plan shall obtain an authorization, which meets the requirements set out in the Plan’s Use of Authorizations Policy and Procedure, from all participants and beneficiaries who will receive or be affected by a communication that meets the definition of “marketing” under the HIPAA privacy rules. The authorization must be signed and received by the Plan before the marketing activity begins (e.g., before a communication is sent to a participant or beneficiary, or before a list of names is send to a third party to market a product or service).

19. Record retention

Policy statement

This policy and procedure is adopted pursuant to various requirements of the privacy rules, including but not limited to Section 164.530(j), under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

This policy specifically focuses on the record retention period requirements specific to the administration of the Plan and, as such, is not meant as an exhaustive list of all record retention requirements to which the Plan may be subject under federal laws other than the Health Insurance Portability and Accountability Act (HIPAA) of 1996. For example, the Plan may have general recordkeeping requirements under the Internal Revenue Code as a taxpayer and under various other federal and state laws as an employer.

HIPAA's privacy rules require that any required documentation must be retained (either in written or electronic form) for six years from the later of the date it was created or the date it was last in effect. Records that must be retained under the HIPAA privacy rules, include, but are not limited to, plan documents, policies on PHI uses and disclosures, signed authorizations, the privacy notice, documentation regarding individual rights and records, and Business Associate contracts.

Procedures

Retention Periods

HIPAA Records	Retention Period
Plan Documents	Current year plus six prior years
Policies on PHI uses and disclosures and minimum necessary uses and disclosures	Current year plus six prior years
• All signed authorizations	Current year plus six prior years
• Notice of Privacy Practices	Current year plus six prior years
Documentation regarding individual rights, including any communication required to be in writing (for example notice of denial of access), and documentation of agreed-upon restrictions on use or disclosure of PHI	Current year plus six prior years
Records of PHI disclosure for non-TPO (treatment, payment or health care operations) purposes	Current year plus six prior years
Individual complaints and their outcome	Current year plus six prior years
Records of sanctions imposed on employees, agents, subcontractors, or Business Associates	Current year plus six prior years
Information on whether an entity is a hybrid or affiliated entity or an organized healthcare arrangement	Current year plus six prior years
Business associate contracts	Current year plus six prior years
Workforce training policies and procedures	Current year plus six prior years
Privacy Official designation	Current year plus six prior years
Breach notification	Current year plus six prior years

20. Administrative, technical, and physical safeguards

Policy statement

This policy and procedure is adopted pursuant to Section 164.530(c) and Section 164.304 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

The Plan will have in place appropriate administrative, technical, and physical safeguards to ensure the privacy and security of PHI and prohibit access to PHI by anyone other than those individuals specifically authorized to work with PHI as part of Plan operations. The Plan will also implement reasonable safeguards to limit incidental and avoid prohibited uses and disclosures.

In determining what is reasonable, the Plan will assess potential risks to privacy, as well as consider such issues as the potential effects on plan treatment, payment, and health care operations, and any administrative or financial burden to be incurred from implementing particular safeguards. The Plan will conduct periodic HIPAA Security Risk Assessments to assist in the development of administrative, technical, and physical safeguards. The following procedures are examples of the types of adjustments or modifications to facilities or systems that may constitute reasonable safeguards, based on the Plan's assessment Policies concerning administrative, technical, and physical safeguards may be published by the Plan from time to time.

Procedures

1. The Plan will implement administrative actions and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the Plan's workforce in relation to the protection of that information.
    a. The Plan will conduct periodic HIPAA Security Risk Assessments as required by law and regulation. to identify vulnerabilities and risks.
    b. The Plan will develop and enforce security policies and procedures.
    c. The Plan will designate a security officer.
    d. The Plan will train employees on security awareness and their obligation to safeguard information.
    e. The Plan will implement access controls and user management.
    f. The Plan will establish an incident response and business continuity plan.
    g. The Plan will create a disaster recovery program for loss of data due to fire, vandalism, natural disaster, or other system failure.
    h. The Plan will document security incidents.
    i. The Plan will designate security protocols for electronic or paper documents (including reporting a breach of confidentiality and disciplinary procedures for employees that breach confidentiality policies).

j. The Plan will adopt a protocol concerning terminated employees to assure data protection.

2. The Plan will implement physical measures, policies, and procedures to protect its electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
   a. The Plan will control physical access to facilities and sensitive areas.
   b. The Plan will implement secure storage for physical media and equipment.
   c. The Plan will control personnel access to sensitive areas, and will implement a visitor access policy.
   d. The Plan will designate security protocols for electronic or paper documents (including reporting a breach of confidentiality and disciplinary procedures for employees that breach confidentiality policies).
   e. The Plan will implement policies for use and storage of paper documents.
   f. After appropriate use is complete, documents containing PHI will be shredded before disposal, subject to the time frames specified in the record retention policy.
   g. Prior to disposal, hard drives of all computers shall be erased so that no Plan data remains and none can be recovered by any known recovery method. If hardware is leased, it shall be wiped prior to being returned to the lessor.
   h. Appropriate precautions will be taken when opening mail to assure that documents containing PHI are secure.

3. The Plan will implement technology and the policy and procedures for its use that protect electronic PHI and control access to it.
   a. The Plan will implement appropriate firewalls to protect information.
   b. The Plan will implement policies concerning the use of email and limit the use of email for transmitting PHI.
   c. The Plan will implement authentication systems, such as log in policies, password policies, and other data protection policies.
   d. The Plan will implement policies governing the use of faxes.
   e. The Plan will implement access control systems including user based, role based or context based access.
   f. The Plan will implement a data loss prevention program.
   g. The Plan will implement policies concerning hardware and mobile devices used by its workforce.
   h. The Plan will implement policies for cloud storage, including assuring a business associate agreement is in place.

21. Privacy official

Policy statement

This policy and procedure is adopted pursuant to Subpart D of Part 164 of Title 45 of the Code of Federal Regulations (Section 164.530), under the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act of 2009. If the breach notification rules are changed by HHS, the Plan will follow the revised rules.

The Plan has designated a privacy official who is responsible for the development and implementation of the privacy policies and procedures of the Plan. In carrying out these duties, the Privacy Official may be responsible for the following tasks:

1. Developing and implementing HIPAA's privacy rules as applicable to the Plan, in coordination with the plan's professional advisors;
2. Monitoring training programs for Plan staff and, where appropriate, service providers, Business Associates and other third parties;
3. Serving as the designated decision maker for issues and questions involving interpretation of the HIPAA privacy rules, in coordination with Legal Counsel;
4. Coordinating HIPAA compliance with the service providers who use and disclose PHI to administer Plan benefits;
5. Developing overall privacy policies and procedures for the plan as well as a notice of privacy practices and forms necessary to implement the Plan's policies;
6. Establishing programs to audit and monitor Business Associates and internal privacy compliance, including the performance of the initial and periodic privacy risk assessments;
7. Cooperating with the Office of Civil Rights or other applicable governmental agency in any compliance review or investigations; and
8. Keeping up to date on the latest privacy and security developments and federal and state laws and regulations.

The Plan has designated **Michael F. Sabitoni** as the Privacy Official.

22. Breach notification

Policy statement

This policy and procedure is adopted pursuant to Subpart D of Part 164 of Title 45 of the Code of Federal Regulations (Section 164.400, et seq.), under the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act of 2009. If the breach notification rules are changed by HHS, the Plan will follow the revised rules.

The Plan will follow this notification procedure to determine if there has been a breach of unsecured PHI and to respond to any such breach. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable through the use of a technology or methodology specified by HHS. At this time, the specified technologies and methodologies are:

- Encryption for electronic PHI "in motion," "at rest" and "in use."
- Hardcopy PHI, whether documents, discs, tapes, flash drives or any other portable technology, is destroyed by shredding.
- Electronic PHI is destroyed in accordance with applicable guidance issued by HHS.

A breach of unsecured PHI means the acquisition, access, use or disclosure of unsecured PHI in a manner that is not permitted by the HIPAA privacy rules, and that compromises the security or privacy of the PHI. However, the following three circumstances are excluded from the definition of a breach:

- An unintentional acquisition, access or use of PHI by a workforce member acting in good faith and within the scope of his or her authority, as long as the acquisition, access or use does not result in further use or disclosure in a manner not permitted by the privacy rule;
- Any inadvertent disclosure of PHI by a workforce member authorized to access PHI to another person who is authorized to access PHI maintained by the Plan, as long as the information received as a result of that disclosure is not further used or disclosure in a manner not permitted by the Privacy Rule;
- A disclosure of PHI where the Plan has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably been able to retain such information.

If the violation does not fit into one of the three exclusions, the Privacy Official will presume that a breach of unsecured PHI has occurred unless a risk assessment, conducted in accordance with these procedures, determines that there is a low probability that the PHI has been compromised. If the Privacy Official determines there has been a breach of unsecured PHI, the Plan will provide notification in accordance with these procedures.

The HIPAA privacy rule's administrative requirements discussed elsewhere in the Plan's HIPAA Privacy Policies and Procedures (e.g., providing training to workforce, having complaint process, applying sanctions for violations, maintaining documentation, etc.) apply to these breach notification requirements.

Business associates

When a Business Associate or a Business Associate's agent/subcontractor is responsible for the breach, the Business Associate is obligated to inform the Plan of the breach as soon as possible but within no longer than 30 days. Upon receipt of such notice, the Plan will determine in each instance whether the required breach notices will be provided by the Plan or by the applicable Business Associate. However, if the Business Associate agreement sets forth a procedure that governs how breach notice will be provided if the Business Associate is responsible for the breach, the provisions of the Business Associate agreement will be followed as long as they are permissible under applicable law.

Procedures

1. Determination of Violation
    a. All members of the Plan's workforce are required to report to the Plan's Privacy Official any use or disclosure of PHI that might be a violation of these Policies and Procedures or the privacy rule. Reports may be made orally or in writing but must be provided immediately upon committing any action that the person believes may have violated the Plan's Policies and Procedures or the privacy rules or immediately upon learning that another member of the workforce or any other person (such as a Business Associate) may have done something in violation of the Plan's Policies and Procedures or the privacy rules.
    b. If the Plan has a cybersecurity service provider that provides services related to the breach, the cybersecurity service provider may provide assistance through the process.
    c. The Privacy Official, or their designee, will:
        1) Accept reports from any person who believes there may have been a violation of the Plan's privacy rules,
        2) Investigate the alleged violation of the Plan's privacy rules,
        3) Determine, in consultation with other workforce members and the Plan's professional advisors, as appropriate, whether there has been a breach of unsecured PHI, as defined in the Plan's Breach Notification Policy Statement and in Section 164.402 (i.e., there has been an acquisition, access, use or disclosure not permitted by the privacy rule that has compromised the security or privacy of the PHI). To make this determination, the Privacy Official may have to conduct a risk assessment as described below in sub-section 4., and
        4) Make and keep a written record of the breach incident investigation and of the determination whether there has or has not been a breach of unsecured PHI.
    d. If the Privacy Official believes that the privacy or security of PHI may not have been compromised, he or she may conduct a risk assessment (after an alleged violation of the privacy rules has been reported and before a Breach Notification is provided to affected individuals) to determine whether there is a low probability that PHI has been compromised. The risk assessment will base its determination on consideration of at least the following factors:
        1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
        2) The unauthorized person who used the PHI or to whom the disclosure was made;
        3) Whether the PHI was actually acquired or viewed; and

4) The extent to which the risk to the PHI has been mitigated.

e. If the risk assessment is not conducted or the Privacy Official determines that there is more than a low probability that PHI has been compromised, a Breach Notification will be provided as set forth in this procedure. If, based on the risk assessment, the Privacy Official determines that there is a low probability that PHI has been compromised, Breach Notification will not be provided.

f. Any records related to the investigation and/or risk assessment will be retained in accordance with the Record Retention policy.

2. Notification to an Individual of a Breach of Unsecured PHI

a. The Plan will, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been — or is reasonably believed to have been — accessed, acquired, used or disclosed as a result of the breach.

b. The Plan will provide the notice to each individual without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. Notification may be delayed at the request of a law enforcement official if the official states that notice would impede a criminal investigation or cause damage to national security.

c. The individual notices will be in writing, in plain language, and will include, to the extent possible, all of the following points:

1) A brief description of what happened (including the date of the breach and the date of the discovery of the breach, if known),

2) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, or other types of information were involved) — without listing the actual individual identifiers or other sensitive information involved,

3) Any steps that individuals should take to protect themselves from potential harm,

4) A brief description of what the Plan is doing to (1) investigate the breach, (2) mitigate harm, and (3) protect against further breaches, and

5) Contact information for individuals to ask questions including a toll-free phone number, an e-mail address, a Web site, or postal address.

d. The Plan will mail these notices, by first-class mail, to the individual's last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, the Plan will provide notice by electronic mail. If the Plan knows the individual is deceased and has the address of next of kin or personal representative, the notice will be mailed to that person.

e. If the Plan has insufficient or out-of-date contact information for fewer than 10 individuals, the Plan will use an alternate form of notice such as telephone. If the Plan has insufficient or out-of-date contact information for 10 or more individuals, the Plan will notify those individuals either through a conspicuous posting on the Plan's Web site for a period of 90 days or conspicuous notice in appropriate major print or broadcast media.

f. In situations deemed urgent by the Plan due to the possible imminent misuse of unsecured PHI, the Plan may provide notice to the affected individual(s) by phone or other means, in addition to providing the individual written notice.

g. If the individual affected by breach is a minor or otherwise lacks legal capacity due to a physical or medical condition, the Plan will provide the notice to the individual's

personal representative (who, in the case of a minor child, will typically be the child's parent).

3. Notification to HHS
    a. For breaches of unsecured PHI that involve fewer than 500 individuals, the Plan will keep a log and report these breaches to HHS on an annual basis, not later than 60 days after the end of each calendar year in which the breaches were discovered by the Plan, in the manner specified on the HHS Web site. The Plan may opt to report breaches to HHS at the same time it sends notices to individuals, in the manner specified on the HHS Web site.
    b. For breaches of unsecured PHI involving 500 or more individuals, the Plan will notify HHS at the same time it provides the individual notices required above, in the manner specified on the HHS Web site. Notification may be delayed at the request of a law enforcement official if the official states that notice would impede a criminal investigation or cause damage to national security.
4. Notification to the Media For Breaches Involving 500+ Individuals

    For breaches involving more than 500 residents of one state or one jurisdiction (i.e., a geographic area smaller than a state, such as a county, city or town), the Plan will notify prominent media outlets serving the state or jurisdiction at the same time it provides the individual notices required above. Notification may be delayed at the request of a law enforcement official if the official states that notice would impede a criminal investigation or cause damage to national security. The Plan must notify the media directly, and not by posting the notification on its website. The Plan is not required to incur any cost to print or run a media notice.
5. Breach by Business Associate
    a. Through its Business Associate agreements or otherwise, the Plan will require its Business Associates to promptly notify the Plan of any breach of unsecured PHI for which the Business Associate or one of its agents/subcontractors is or may be responsible.
    b. Through its Business Associate agreement or otherwise, the Plan will determine whether any required notices will be provided by the Plan or by the applicable Business Associate.
6. Documentation
    a. The Plan will maintain documentation sufficient to demonstrate that, for each incident, (1) the requisite investigation and/or risk assessment was conducted, and (2) that all required notifications were provided or the use or disclosure at issue did not constitute a breach of unsecured PHI (and thus no notifications were required).
    b. The Plan will maintain such documentation in accordance with the Records Retention Policy.

23. Limitations on use and disclosure of genetic information

Policy statement

This policy and procedure is adopted pursuant to Section 164.502(a)(5)(i) under the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by Health Information Technology for Economic and Clinical Health Act (HITECH) and the Genetic Information Non-Discrimination Act of 2008. If the privacy rules are changed by HHS, the Plan will follow the revised rules.

The Plan will not use or disclose PHI that is genetic information for underwriting purposes.

Genetic information includes, with respect to an individual, information about:

- The individual's genetic tests;
- The genetic tests of the individual's family members;
- The manifestation of a disease or disorder in family members (described below) of such individual; or
- Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member (described below) of the individual.

References to "family members" include: parents, spouses, siblings, children, grandparents, grandchildren, aunts, uncles, nephews, nieces, great-grandparents, great-grandchildren, great aunts, great uncles, first cousins, great-great grandparents, great-great grandchildren and children of first cousins, whether by consanguinity (such as siblings who share both parents) or affinity (such as by marriage or adoption). In addition, references to genetic information of an individual or family member includes the genetic information of a fetus carried by the individual or family member, and any embryo legally held by an individual or family member using assisted reproductive technology.

Underwriting purposes is defined broadly to include:

- Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of coverage for, benefits under the Plan. Among other items, this includes 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;
- The computation of premium or contribution amounts under the Plan. Among other items, this includes discounts, rebates, payment in kind or any other premium differential mechanisms in return for completing a health risk assessment or participating in a wellness program;
- Other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits; and
- Underwriting purposes do not include determinations of medical appropriateness where an individual seeks a benefit under the Plan.

24. Right to request restrictions on use and disclosure

Policy statement

This policy and procedure is adopted pursuant to Section 164.522 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

A covered individual may request that the Plan restrict the use and disclosure of PHI for treatment, payment, and heath care operations and to persons involved in an individual's care and for notification purposes.

The Plan, however, is not required to agree to the request if the Privacy Official (or the Privacy Official's designee) determines it to be unreasonable, for example, if it would interfere with the Plan's ability to pay a claim.

If the Plan agrees to the requested restriction, it will abide by the restriction except:

1. If the individual is in need of emergency treatment; **and**
2. The disclosure is necessary to provide that treatment.

The Plan may then use the restricted PHI, and may disclose this information to a health care provider in order to provide the needed treatment.

If restricted PHI is disclosed to a health care provider because it is necessary for emergency treatment, the Plan will request that the health care provider not further use or disclose the information.

The Plan's agreement to a restriction on the use or disclosure is not effective to prevent uses or disclosures:

1. When required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine compliance with HIPAA;
2. For Facilities directories; or
3. For instances where an authorization is not required under the Plan's Policy for Disclosure of PHI for Public Health, Law Enforcement or Legal Process.

The Plan's agreement to a restriction is binding only on the Plan and its Business Associates, not on other entities such as insurers or health care providers.

Business associates

As Business Associate Agreements are negotiated and a Business Associate takes responsibility for Individual Rights under this Policy, this Policy and Procedure will incorporate policies of the applicable Business Associate by reference.

Procedures

1. An individual covered by the Plan may request that the Plan restrict any use or disclosure of his/her PHI for treatment, payment, and health care operations, and to persons involved in an individual's care and for notification purposes.
2. To restrict the use or disclosure of PHI, an individual must make a written request to the Plan.
3. The Privacy Official (or the Privacy Official's designee) will review the request and notify the covered individual in writing of the decision within 30 days.
4. The Plan's agreement to a restriction on the use or disclosure will not prevent uses or disclosures:
    a. When required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine compliance with HIPAA;
    b. For Facilities directories; or
    c. For instances where an authorization is not required under the Plan's Policy for Disclosure of PHI for Public Health, Law Enforcement or Legal Process.
5. The covered individual may revoke his/her agreement to restrict the use and disclosure of PHI by submitting a signed written request to terminate the agreement.
6. The Plan may terminate an agreement to restrict the use and disclosure of PHI by notifying the covered individual in writing. The termination will only be effective for PHI created or received after the date the Plan sends the notice.
7. The Privacy Official (or the Privacy Official's designee) will retain documentation of the restrictions that are approved for six years.

25. Right to request confidential communications be transmitted by alternative means

Policy statement

This policy and procedure is adopted pursuant to Section 164.522(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

The Plan will permit and accommodate a covered individual's reasonable request to have PHI sent by alternative means or to an alternative location. A request by a covered individual must contain a statement that disclosure of the PHI may endanger the covered individual.

Business Associates

As Business Associate Agreements are negotiated and a Business Associate takes responsibility for Individual Rights under this Policy, this Policy and Procedure will incorporate policies of the applicable Business Associate by reference.

Procedures

1. A covered individual may request the Plan to transmit PHI by an alternative means or to an alternative location.
2. The request must be in writing in a form and method prescribed by the Plan.
3. The Privacy Official (or the Privacy Official's designee) will review and notify the covered individual within 30 days as to whether the request will be honored.
4. The Plan will only accommodate a reasonable request. A request will be considered reasonable if the request is for mailing to a different address or allowing the covered individual to personally pick up information that would otherwise be mailed. The alternative address or request to allow a pickup must be specified in the request.

26. Right of access to PHI

Policy statement

This policy and procedure is adopted pursuant to Section 164.524 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

A covered individual has the right to inspect and obtain a copy of PHI pertaining to the individual in a designated record set, except as otherwise provided in the law or provided in the Plan's Procedures for the Right of Access to PHI. The Plan may impose a reasonable cost-based fee for copying PHI or for preparing a summary of PHI.

The Plan will provide access to PHI only for as long as the PHI is maintained in a designated record set.

Business associates

As Business Associate Agreements are negotiated and a Business Associate takes responsibility for Individual Rights under this Policy, this Policy and Procedure will incorporate policies of the applicable Business Associate by reference.

Procedures

1. A covered individual under the Plan or a personal representative of such individual may request the right to inspect and/or copy PHI pertaining to the covered individual in a designated record set.
2. "Designated record set" means a group of records maintained by or for the Plan that is: (1) The medical records and billing records about individuals maintained by or for a covered health care provider; (2i) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for the Plan; or (3) Used, in whole or in part, by or for the Plan to make decisions about individuals.

   The term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the Plan.

   In general, all records maintained by the Plan relating to the covered individual's enrollment, eligibility, claims, appeals, and related information are considered to be part of the designated record set for an individual. It shall not include records related to claims audits. The Privacy Official (or the Privacy Official's designee) shall have ultimate responsibility for determining what constitutes the designated record set.
3. The following information will not be considered part of the designated record set made available for inspection or copying. Requests for access to this information will be denied:
   a. Psychotherapy notes;
   b. Copies of health information kept in multiple locations (only the original should be included in the designated record set);

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

d. PHI maintained by the Plan that is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law or exempt for Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 493.3(a)(2);

e. PHI that was obtained under a promise of confidentiality (other than from a health care provider), where the access requested would be reasonably likely to reveal the source of the information;

f. Quality improvement or risk management records;

g. Research documentation while a clinical trial is taking place, if the individual who is part of the clinical trial agreed to denial of access upon participation;

h. Appointment schedules;

i. Information compiled in anticipation of a government or administrative proceeding; and

j. Cancer registry information.

Any documents contained in a file that are not part of the Designated Record Set will be clearly identified as “Not Part of Designated Record Set.”

4. The Plan will also deny the right to inspect and copy the PHI, if in the opinion of a licensed health care professional, the access requested by the individual or their personal representative, is reasonably likely to cause substantial harm to the individual or another person. The Plan will also deny the right to inspect and copy PHI that makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to such other person.

5. Review of a Denial of Access. If access is denied for the reasons stated in paragraph four, the individual has the right to have the denial promptly reviewed by a licensed health care professional designated as a reviewing official who did not participate in the original decision. The Plan will designate an unrelated and different licensed health care professional to act as the reviewing official in such cases. Denials of access for the reasons set out in paragraph three are not subject to review. The Plan will provide a written notice to the individual of a determination on review.

6. Form of Request. A request to inspect and/or copy PHI must be made on a form provided by the Plan and mailed to the Plan’s address Form. All requests are subject to the Plan’s Verification Policy.

7. The form requesting the right to inspect and/or copy will be date-stamped by the Privacy Official (or the Privacy Official’s designee) and will be logged in.

8. If a personal representative makes the request, there must be a proper authorization on file pursuant to the Plan’s Personal Representative Authorization Policy.

9. Time for Responding to Request. The Privacy Official (or the Privacy Official’s designee) will act on a properly filed request within 30 days of receipt of the request (60 days if the PHI is not maintained on-site).

   a. If the request is approved, the individual will be notified of the approval and access will be provided.

b. If the request is denied, a written denial notice will be provided stating the basis for denial. For a denial notice concerning a denial for the reasons stated in paragraph 4, the Plan will also provide a statement of the right of the individual to have the denial reviewed and a description of how the individual may file a complaint with the Plan and the U.S. Department of Health and Human Services.

c. The time for responding may be extended by 30 days if the Privacy Official (or the Privacy Official's designee) is unable to act upon the request and the individual is notified in writing of the need for extension within 30 days of receipt of the request.

d. If the Plan does not maintain the PHI that is the subject of the request, and the Plan knows where the requested information is maintained, it will inform the individual where to direct the request for access in the response to the request.

10. Providing the Access Requested. The Plan will provide the individual with access to the PHI in a timely manner in the form or format requested by the individual, if it is readily producible in such form or format; or if not, in a readable hard copy form or such other form or format as agreed to by the Plan and the individual. In lieu of providing PHI, the Plan may provide a summary of the PHI requested if the individual agrees in advance to the summary and to any fees charged for the summary. The Plan may arrange with the individual for a convenient time or place to inspect or obtain a copy of the information, or mail a copy of the information at the individual's request.

11. Fees. The Plan may charge the following fees:
    a. Costs of copying PHI including labor and supplies;
    b. Postage for mailing the PHI; and
    c. The cost of preparing a summary of PHI.

12. Documentation. The Plan will document the designated record set that is subject to access by individuals. It will also document the title of the individual responsible for receiving and processing requests for access by individuals. The Plan will also maintain any communication required by this procedure to be in writing (e.g., notice of denial).

27. Right to amend PHI

Policy statement

This policy and procedure is adopted pursuant to Section 164.526 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

A covered individual has the right to have the Plan amend PHI or other information maintained in its designated record set subject to the exceptions set out in the Plan's Right to Amend PHI Procedures. If the Plan does not agree to amend the PHI, the individual has the right to submit a written statement disagreeing with the denial and explaining the basis for the disagreement. The Privacy Official (or the Privacy Official's designee) may then issue a rebuttal statement.

The right to amend PHI applies only for as long as the PHI is maintained in a designated record set.

The Plan is not required to delete or expunge any PHI from its records under the HIPAA privacy rules. In addition, the Plan's right to amend does not include the right for a covered individual to make the actual changes to PHI. Where a request to amend is accepted by the Plan, the Plan will determine the appropriate amendment (taking into account any suggested amendment from the individual).

Business associates

As Business Associate Agreements are negotiated and a Business Associate takes responsibility for Individual Rights under this Policy, this Policy and Procedure will incorporate policies of the applicable Business Associate by reference.

Procedures

1. A covered individual may request the Plan to amend PHI pertaining to that individual. The PHI must be in a designated record set maintained by the Plan.
2. "Designated record set" means a group of records maintained by or for the Plan that is: (1) The medical records and billing records about individuals maintained by or for a covered health care provider; (2) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for the Plan; or (3) Used, in whole or in part, by or for the Plan to make decisions about individuals.

   The term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the Plan.

   In general, all records maintained by the Plan relating to the covered individual's enrollment, eligibility, claims, appeals, and related information are considered to be part of the designated record set for an individual. It shall not include records related to claims audits. The Privacy Official (or the Privacy Official's designee) shall have ultimate responsibility for determining what constitutes the designated record set.

3. The following information will not be considered part of the designated record set made available for inspection or copying. Requests for amendment to this information will be denied:
    a. Psychotherapy notes;
    b. Copies of health information kept in multiple locations – only the original should be included in the designated record set;
    c. Information compiled in anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
    d. PHI maintained by the Plan that is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or exempt for Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 493.3(a)(2);
    e. PHI that was obtained under a promise of confidentiality (other than from a health care provider), where the access requested would be reasonably likely to reveal the source of the information;
    f. Quality improvement or risk management records;
    g. Research documentation while a clinical trial is taking place, if the individual who is part of the clinical trial agreed to denial of access upon participation;
    h. Appointment schedules;
    i. Information compiled in anticipation of a government or administrative proceeding;
    j. Cancer registry information.

    Any documents contained in a file that are not part of the Designated Record Set will be clearly identified as “Not Part of Designated Record Set.”
4. A request must be in writing, provide a reason for the request, and be mailed to the following address:
5. Timing of Decision. The Plan will act on the request within 60 days of receipt of the request. The Plan may extend the time to comply by 30 days, provided that the Plan notifies the individual in writing within the first 60 days and explains the reasons for the delay and the date by which the Plan will act.
6. Reason for Denial. The Plan will deny the request for amendment if the Privacy Official (or the Privacy Official’s designee) determines that the PHI or other record:
    a. Was not created by the Plan, unless the individual provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the request;
    b. Is not part of the designated record set;
    c. Is not available for inspection under HIPAA (pursuant to the Plan’s Policy for Rights of Access to PHI); or
    d. Is accurate and complete.

7. Accepting the Amendment. If the Plan accepts the request for the amendment in whole or in part, then the Plan will do the following:
    a. Make the appropriate amendment to PHI by providing a link to the affected records or append the affected records within 60 days of the receipt of the request;
    b. Within 60 days of the receipt of the request, inform the individual of the amendment that will be made and obtain from the individual the identification of and an agreement to have the Plan notify persons who should be aware of the amendment; and
    c. Make reasonable efforts to provide the amendment to persons identified by the individual or persons, including Business Associates that the Plan knows may have or could rely on the PHI to the detriment of the individual.
8. Denying the Amendment. If the request to amend is denied, in whole or in part, the Privacy Official (or the Privacy Official's designee) will provide a denial notice containing the following information (See *Denial of Request to Amend Protected Health Information Form*):
    a. Basis for denial;
    b. A statement of the individual's right to submit a statement of disagreement with the denial, including information on how this statement can be filed;
    c. A statement that if an individual does not submit a statement of disagreement, the individual has a right to request that the Plan furnish a copy of the Request for amendment and Denial of the request with future disclosures of the PHI that was the subject of the request; and
    d. A description of how an individual can file a Complaint with the Plan and the U.S. Department of Health and Human Services.
9. Statement of Disagreement. Where the request to amend is denied, the individual may submit a written statement disagreeing with the denial and explaining the basis for the disagreement. Such a statement cannot exceed three (3) pages (or other reasonable limit).
10. Rebuttal Statement. The Plan, through its Privacy Official (or the Privacy Official's designee), may then issue a written rebuttal to the individual's statement of disagreement. If the Plan prepares a rebuttal statement, a copy of the rebuttal will be provided to the individual who submitted the statement of disagreement.
11. Recordkeeping. The request for amendment, the denial, any statement of disagreement, and any rebuttal statement will be linked or appended to the related PHI kept in the designated record set.
12. Future Disclosures.
    a. If a statement of disagreement has been submitted, the statement or a summary of the statement will be attached to any subsequent disclosure of the PHI.
    b. If a statement of disagreement has not been submitted, then the Plan will include (upon the individual's request) the individual's request for amendment and the denial (or a summary of this information) with any subsequent disclosure of the PHI.
    c. When a subsequent disclosure is made in the form of an electronic transmission that is a standard transaction under HIPAA's Electronic Data Interchange ("EDI") rules, the required information will be sent separately to the recipient of the information, if the transaction does not permit the additional material to be included with the disclosure.

13. Action on Amendment Made by Other Covered Entities. Upon notification of an amendment to PHI by another covered entity (e.g., another health plan or medical provider), the Plan will amend the PHI in its designated record set.

14. Documentation. The Plan will document the designated record set that is subject to access by individuals. It will also document the title of the individual responsible for receiving and processing requests for access by individuals. The Plan will also maintain any communication required by this procedure to be in writing (e.g., notice of denial).

28. Right to accounting of disclosures of PHI

Policy statement

This policy and procedure is adopted pursuant to Section 164.528 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the HIPAA privacy rules are changed by the Department of Health and Human Services, Plan will follow the revised rules.

1. A covered individual has the right to request and receive an accounting of disclosures of that individual's PHI made by the Plan in the six years before the date of the request, including the following disclosures:
    a. Uses and disclosures not according to policy by a workforce member or Business Associate;
    b. Disclosures that do not require an authorization under the Plan's Policy for Disclosure of PHI for Public Health, Law Enforcement or Legal Process; and
    c. Federal and state-mandated disclosures, such as Tumor Registry, FDA Adverse Reaction, etc.
2. The following disclosures need not be accounted for:
    a. Disclosures of PHI for treatment, payment, or health care operations;
    b. Disclosures to the covered individual;
    c. Disclosures for national security or intelligence purposes;
    d. Disclosures to correctional institutions or law enforcement officials having lawful custody of an inmate as provided under the HIPAA privacy rules;
    e. Disclosures before the compliance date of the HIPAA privacy rules (April 14, 2003);
    f. Disclosures made pursuant to a valid authorization;
    g. Disclosures incident to a use or disclosure otherwise permitted or required by HIPAA;
    h. Disclosures that are part of a "limited data set" as described in section 164.514(e) of the HIPAA privacy rules; and
    i. Disclosures for facilities directories or to persons involved in the individual's care or other notification purposes.

Business associates

As Business Associate Agreements are negotiated and a Business Associate takes responsibility for Individual Rights under this Policy, this Policy and Procedure will incorporate policies of the applicable Business Associate by reference.

Procedures

Accounting Request Form

1. An individual who requests an accounting must use the form entitled Individual Request for Accounting of Disclosures of Protected Health Information ("Accounting Request Form").
2. The Privacy Official (or the Privacy Official's designee) will provide an Accounting Request Form to any individual who wishes to request an accounting of disclosures.

3. The Accounting Request Form must be completed and signed by the individual. The individual may mail, fax, or deliver the Accounting Request Form to the Privacy Official at the following address:

   Michael F. Sabitoni
   Laborers' Local 271
   410 South Main Street
   Providence, RI 02903

Response to request

1. The Privacy Official (or the Privacy Official's designee) will review the Accounting Request Form and prepare a written Accounting of all uses and disclosures for which Accounting is required under the Plan's Right to Accounting Policy.
2. The Privacy Official (or the Privacy Official's designee) will respond as follows:
   a. An Accounting will be provided within sixty days of receipt of the Request for Accounting Form by the Privacy Official.
   b. If the Plan is unable to provide the Accounting within 60 days, the Plan will invoke one thirty-day extension, provided the individual is notified by the Privacy Official (or the Privacy Official's designee) in writing within the first 60 days of the reason for the delay and the date by which the Plan will provide the accounting.
   c. Upon request, one Accounting for an individual in a twelve-month period will be provided without charge. The Plan will impose a fee based on labor and supplies for each additional request during the twelve-month period. However, the Privacy Official (or the Privacy Official's designee) will notify the individual of the fee in advance and allow the individual to modify or withdraw the request.

Exceptions to the accounting requirement

1. The accounting requirement does not apply to disclosures set out in section 2 of the Plan's Right to Accounting Policy.
2. The Plan will temporarily suspend the individual's right to receive an Accounting of such uses and disclosures to a health oversight agency ("agency') or law enforcement official ("official") if a temporary suspension is requested by the agency or official in accordance with the following procedures:
   a. The agency or official states in writing to the Plan that providing such Accounting to the individual would be reasonably likely to impede the agency's activities and specifies the period of time for which the suspension of the right to an Accounting of these disclosures is required; or
   b. The agency or official orally states to the Plan that providing such Accounting to the individual would be reasonably likely to impede the agency's activities and specifies the period of time for the suspension. The Plan will document the statement (including the identity of the agency or official making the statement) and will limit the temporary suspension to no longer than 30 days from the date of the oral statement (unless a written statement complying with the requirements of paragraph (a) is submitted).

Information to be provided in an accounting

1. With the exception of uses and disclosures of PHI that are not subject to an Accounting in accordance with the Plan's Right to Accounting Policy, the Plan will include in an Accounting any uses and disclosures of PHI made during the six years before the date of the Accounting (or fewer years if the Plan's HIPAA compliance date is fewer than six years before the Accounting).
2. Disclosures made to or by Business Associates of the Plan will be included in the Accounting unless such disclosures fall into one of the exceptions for the right to an accounting.
3. For each disclosure, the Accounting will include:
    a. The date of the disclosure,
    b. The name of the entity or person who received the PHI and, if known, the address of the entity or person,
    c. A brief description of the PHI disclosed, and
    d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the written request for disclosure, if any.
4. To the extent that the Plan has made multiple disclosures of PHI to the same person or entity for a single purpose, the Accounting regarding this multiple disclosure will provide:
    a. All information that would be otherwise required for the first disclosure in the Accounting period;
    b. The frequency, periodicity or number of disclosures made during the Accounting period; and
    c. The date of the last such disclosure in the Accounting period.
5. To the extent that the Plan has made disclosures for research purposes (under section 164.512(i) of the HIPAA privacy rules) for 50 or more individuals, the Accounting will provide:
    a. The name of the protocol or research activity;
    b. A plain language description of the protocol or research activity (including the purpose of the research and the criteria for selecting particular records);
    c. The type of PHI disclosed;
    d. The date or period during which the disclosures occurred;
    e. The name, address, and phone number of the entity that sponsored the research and the researcher to whom the PHI was disclosed; and
    f. A statement that PHI may or may not have been disclosed for a particular protocol or research purpose.
6. If the Plan provides an accounting for research purposes under section 5 above, and if it is reasonably likely that this PHI was disclosed for such research, protocol, or activity, the Plan will, upon the individual's request, assist in contacting the entity that sponsored the research and the researcher.

Documentation

The Plan will keep any information that is the subject of an accounting and any written accounting according to its Record Retention policy.