Privacy, Use, and Disclosure Policy (HIPAA)

Innermark

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and its implementing regulations, provides restrictions on the use and disclosure of protected health information (PHI).

Purpose

This policy specifies the responsibilities, requirements, and procedures for the safeguarding, use, and disclosure of protected health information (PHI) transmitted or maintained in any form or medium (electronic or otherwise) by Innermark and its members.

Definitions

Business Associate. An entity, not a member of the Covered Entity's workforce, who:

- Performs or assists in performing a function or activity regulated by HIPAA, on behalf of a covered entity, involving the creation, receipt, maintenance, or transmission (i.e., use and disclosure) of PHI (including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing); or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI;
- Business Associates include:
- A health information organization;
- An e-prescribing gateway;
- Any entity that provides data transmission services with respect to PHI to a covered entity and that requires routine access to PHI;
- An entity that maintains PHI for a covered entity, whether or not the entity actually reviews the PHI.

De-identified Information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified:

- Professional statistical analysis
- Removing 18 specific identifiers.

Designated Record Set. A group of records maintained by or for a company that includes:

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

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

Health Care Operations. Health care operations means any of the following activities to the extent that they are related to Plan administration:

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

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

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

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

Scope

Innermark is a business entity that is considered to be a **BUSINESS ASSOCIATE** with respect to protected health information (PHI), as provided by the standards, requirements, and implementation specifications of HIPAA Privacy Rule. Therefore, this policy applies to Innermark and all the members of its workforce with access to PHI. Additionally, all third parties, subcontractors, or vendors that provide services to Innermark that involve the creation, receipt, maintenance, or transmission of private health information on behalf of the Employer to fulfill its contractual duties, must comply fully with HIPAA's requirements.

Roles and Responsibilities

Privacy personnel designations will be documented and maintained in written or electronic form for six years from time of designation.

(CE) Innermark's **President** will serve as the Privacy Official, who will be responsible for:

- Developing and implementing privacy policies and procedures
- Developing a program to manage complaints
- Appointing personnel who will serve as contact persons to respond to questions, concerns, or complaints about individual PHI privacy and protection
- Ensuring compliance with the HIPAA Privacy Rule regarding Business Associates, Business Associate Agreements (BAA)
- Monitoring compliance of all Business Associates with the HIPAA Privacy Rule, and this policy
- Developing privacy training schedules and programs

Documentation

This policy and associated procedures are designed to ensure compliance as it applies to Innermark, its size, and the type of activities it performs. As documented, this policy will be maintained for at least six years from the date last in

effect. Any necessary or appropriate changes to this policy will be:

- In line with the standards set forth in the HIPAA Privacy Rule;
- To comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations);
- Promptly implemented and documented;
- Reflected in the notice of privacy practices; and
- Communicated, if required, in writing or electronically, and documented.

The Plan shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

General Policy (For Covered Entities - § 164.530)

Training

Innermark will ensure that all personnel are trained on the company's privacy policies and procedures, and the HIPAA Privacy Rule as applicable, annually. The training will be reviewed and updated as needed, but annually at the least.

Administrative, Technical and Physical Safeguards and Firewall

Innermark has appropriate administrative, technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements (see company information security policies and procedures, and controls in place).

- Administrative safeguards include implementing procedures for use and disclosure of PHI, as outlined in this policy.
- Technical safeguards include limiting access to information by creating computer firewalls, which will ensure that there is only authorized access to PHI at the minimum level necessary for administrative functions
- Physical safeguards include locking doors or filing cabinets

Privacy Notice

Innermark's privacy notice will include:

- Uses and disclosures of PHI that may be made by the Innermark;
- Individual's rights under the HIPAA privacy rules;
- Innermark's legal duties with respect to the PHI
- Notification of access to PHI in connection with administrative functions;
- Complaint procedures; and,
- Other information as required by the HIPAA privacy rules.

Innermark will deliver or make available the privacy notice to appropriate individuals:

- Upon request
- Within 60 days after a material change to the notice
- At least once every three years in compliance with the HIPAA Privacy Rule.

Sanctions

Violation of this policy or HIPAA Privacy Rule will be met with sanctions in accordance with Innermark's discipline policy, up to and including termination (*See Information Security Policy*).

Mitigation of Inadvertent PHI Disclosures

Innermark will, to the extent possible, mitigate any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of HIPAA or the policies and procedures set forth in this Policy. As a result, personnel will immediately contact the Privacy Official for the appropriate steps to mitigate the harm to impacted individuals, if the member becomes aware of:

- A disclosure of PHI, either by an employee or a business associate
- An employee or business associate that is not in compliance with this policy or HIPAA

No Intimidation or Retaliatory Acts

No Innermark member may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

No Waiver of HIPAA Privacy

No individual will be required by Innermark or any of its members to waive his or her privacy rights under HIPAA, as a condition of treatment, payment, enrollment or eligibility under a health plan.

Policy and Procedures for Use and Disclosure of PHI

Compliance

All members of Innermark with access to PHI must comply with this Policy and included procedures.

Access to PHI Is Limited to Certain Employees

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

- Any employee who performs functions directly on behalf of Innermark
- Any other employee who has access to PHI on behalf of the Employer for its use in "plan administrative functions".

Employees with access may use and disclose PHI for company administrative functions, and they may disclose PHI to other employees with access for administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and any associated procedures.

Permitted Uses and Disclosures for Plan Administration Purposes

- Innermark may disclose the following for its use:
- (a) de-identified health information;
- (b) Enrollment information;
- (c) summary health information for the purposes of obtaining premium bids for providing health insurance coverage under a plan or for modifying, amending, or terminating the plan; or,
- (d) PHI pursuant to an authorization from the individual whose PHI is disclosed.

PHI may be disclosed to the following employees who have access to use and disclose PHI to perform functions on

behalf of Innermark or to perform plan administrative functions (“employees with access”):

Permitted Uses and Disclosures: Payment and Health Care Operations

PHI may be disclosed for the purposes of Innermark’s own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity. Same stands for disclosure for health care operations. PHI may be disclosed to another covered entity for purposes of the other covered entity’s quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

- Uses and Disclosures for Innermark's Own Payment Activities or Health Care Operations. An employee may use and disclose PHI to perform the Innermark’s own payment activities or health care operations.
    - Disclosures must comply with the "Minimum-Necessary” Standard. (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Official.)
    - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

- Disclosures for Another Entity's Payment Activities. An employee may disclose PHI to another covered entity or health care provider to perform the other entity's payment activities. These disclosures will be made according to procedures developed by the Privacy Official.
- Disclosures for Certain Health Care Operations of the Receiving Entity. An employee may disclose PHI for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the individual and the PHI requested pertains to that relationship. Such disclosures are made according to procedures developed by the Privacy Official.
    - The disclosure must be approved by the Privacy Official.
    - Disclosures must comply with the “minimum-Necessary Standard.”
    - Disclosures must be documented in accordance with the procedure for “Documentation Requirements.”

- Use or Disclosure for Purposes of Non-Health Benefits. Unless an authorization from the individual (as discussed in "Disclosures Pursuant to an Authorization") has been received, an employee may not use a participant's PHI for the payment or operations of the Employer's "non-health" benefits (e.g., disability, worker's compensation, and life insurance). If an employee requires a participant's PHI for the payment or health care operations of non-Plan benefits, follow the steps provided by the Privacy Official.
    - Obtain an Authorization. First, contact the Privacy Official to determine whether an authorization for this type of use or disclosure is on file. If no form is on file, request an appropriate form from the Privacy Official. Employees shall not attempt to draft authorization forms. All authorizations for use or disclosure for non-Plan purposes must be on a form provided by (or approved by) the Privacy Official.
    - Questions? Any employee who is unsure as to whether a task he or she is asked to perform qualifies as a payment activity or a health care operation of the Plan should contact the Privacy Official or his or her designated representative.

No Disclosure for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the Innermark’s “non-health” benefits (e.g., disability, workers’ compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in “Disclosures Pursuant to an Authorization”) or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

Mandatory Disclosures: Individual and HHS

A participant’s PHI must be disclosed as required by HIPAA in three situations: (1) The disclosure is to the individual

who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows); (b) the disclosure is required by law; or, (c) the disclosure is made to HHS for purposes of enforcing HIPAA.

- Request From Individual. Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own PHI, the employee must follow the procedure for "Disclosures to Individuals Under Right to Access Own PHI."
- Request From HHS. Upon receiving a request from a HHS official for disclosure of PHI, the employee must take the steps established by the Privacy Official.
- Follow the procedures for verifying the identity of a public official set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Permissive Disclosures: Legal and Public Policy Purposes

An employee who receives a request for disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Disclosures Covered" must contact the Privacy Official. Disclosures must: (1) be approved by the Privacy Official; (2) comply with the "Minimum-Necessary Standard"; and, (3) be documented in accordance with the procedure for "Documentation Requirements". Permitted disclosures include:

- Disclosures about victims of abuse, neglect or domestic violence, if the following conditions are met:
    - The individual agrees with the disclosure; or
    - The disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and information will not be used against the individual and is necessary for an imminent enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

- For Judicial and Administrative Proceedings, in response to:
    - An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); and
    - A subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, upon receipt of assurances that the individual has been given notice of the request, or that the party seeking the information has made reasonable efforts to receive a qualified protective order.

- To a Law Enforcement Official for Law Enforcement Purposes, under the following conditions:
    - Pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.
    - Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.
    - Information about a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in the best interest of the individual.
    - Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.
    - Information that constitutes evidence of criminal conduct that occurred on the Employer's premises.

- To Appropriate Public Health Authorities for Public Health Activities.
- To a Health Oversight Agency for Health Oversight Activities, as authorized by law.
- To a Coroner or Medical Examiner About Decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law.

- For Cadaveric Organ, Eye or Tissue Donation Purposes, to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation.
- For Certain Limited Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.
- To Avert a Serious Threat to Health or Safety, upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.
- For Specialized Government Functions, including disclosures of an inmate's PHI to correctional institutions and disclosures of an individual's PHI to an authorized federal Official for the conduct of national security activities.
- For Workers' Compensation Programs, to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

Disclosures Pursuant to an Individual Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by an individual. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

Any requested disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required in this policy may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."
- All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.
- Verify that the authorization form is valid. Valid authorization forms are those that:
    - Are properly signed and dated by the individual or the individual's representative;
    - Are not expired or revoked [the expiration date of the authorization form must be a specific date (such as July 1, 2010) or a specific time period (e.g., one year from the date of signature), or an event directly relevant to the individual or the purpose of the use or disclosure (e.g., for the duration of the individual's coverage)];
    - Contain a description of the information to be used or disclosed;
    - Contain the name of the entity or person authorized to use or disclose the PHI;
    - Contain the name of the recipient of the use or disclosure;
    - Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and
    - Contain a statement regarding the possibility for a subsequent re-disclosure of the information.

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

Verification of Identity of Those Requesting Protected Health Information

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

- **Request Made by Individual.** When an individual requests access to his or her own PHI, the following steps should be followed:
    - Request a form of identification from the individual. Employees may rely on a valid driver's license, passport or other photo identification issued by a government agency.
    - Verify that the identification matches the identity of the individual requesting access to the PHI. If

you have any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.
    - Make a copy of the identification provided by the individual and file it with the individual's designated record set.
    - If the individual requests PHI over the telephone, ask for his or her social Security number.
    - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

- **Request Made by Parent Seeking PHI of Minor Child.** When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:
    - Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.
    - Disclosures must be documented in accordance with the procedure "Documentation Requirements."

- **Request Made by Personal Representative.** When a personal representative requests access to an individual's PHI, the following steps should be followed:
    - Require a copy of a valid power of attorney or other documentation—requirements may vary state-by-state. If there are any questions about the validity of this document, seek review by the Privacy Official.
    - Make a copy of the documentation provided and file it with the individual's designated record set.
    - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

- **Request Made by Public Official.** If a public official requests access to PHI, and if the request is for one of the purposes set forth above in "Mandatory Disclosures of PHI" or "Permissive Disclosures of PHI," the following steps should be followed to verify the official's identity and authority:
    - If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set.
    - If the request is in writing, verify that the request is on the appropriate government letterhead.
    - If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
    - Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Legal Department.
    - Obtain approval for the disclosure from the Privacy Official.
    - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

- **Requests for Disclosure of PHI From Spouses, Family Members, and Friends.** PHI will not be disclosed to family or friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member or friend, will be able to access PHI.
    - If an employee receives a request for disclosure of an individual's PHI from a spouse, family member or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information."
    - Once the identity of a parent or personal representative is verified, then follow the procedure for "Individual’s Request for Access."
    - All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for "Disclosures Pursuant to Individual Authorization."

Disclosures of PHI to Business Associates

Business Associate is an entity that:

- performs or assists in performing a Plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or,
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Business Associates include:

- health information organizations;
- e-prescribing gateways;
- other entities that provide data transmission services with respect to PHI and require routine access to PHI;
- entities that offer a personal health record to one or more individuals on behalf of a covered entity; or
- entities that maintain PHI, whether or not the entities actually review the PHI.

Employees may disclose PHI to Innermark's business associates and allow the business associates to create or receive PHI on its behalf. However, prior to doing so, Innermark will first obtain assurances from the business associate that it will appropriately safeguard the information. All uses and disclosures by a "business associate" will be made in accordance with a valid business associate agreement. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Official and verify that a business associate contract is in place.

The following additional procedures must be satisfied:

- Disclosures must be consistent with the terms of the business associate contract.
- Disclosures must comply with the "Minimum-Necessary Standard." (Under that procedure, each recurring disclosure will be subject to a separate policy to address the minimum-necessary requirement, and each non-recurring disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

- Procedures for Disclosures
    - Identify recurring disclosures. For each recurring disclosure, identify the types of PHI to be disclosed, the types of person who may receive the PHI, the conditions that would apply to such access, and the standards for disclosures to routinely-hired types of business associates. Create a policy for each specific recurring disclosure that limits the amount disclosed to the minimum amount necessary to accomplish the purpose of the disclosure.
    - For all other requests for disclosures of PHI, contact the Privacy Official, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

- Procedures for Requests
    - Identify recurring requests. For each recurring request, identify the information that is necessary for the purpose of the requested disclosure and create a policy that limits each request to the minimum amount necessary to accomplish the purpose of the disclosure.
    - For all other requests for PHI, contact the Privacy Official, who will ensure the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

- Exceptions

- The "minimum-necessary" standard does not apply to any of the following:
- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to an individual authorization;
- Disclosures made to HHS;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

Disclosures of De-Identified Information

De-identified information is not PHI; it is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways to determine that information is de-identified: either by professional statistical analysis, or by removing specific identifiers.

Upon approval and verification from the Privacy Official that the information in question is de-identified, the de-identified information may be used and disclosed freely in accordance with HIPAA privacy regulations.

Individual's Request for Access

HIPAA provides individuals the right to access and obtain copies of their PHI (or electronic copies of PHI) that Innermark (or its business associates) maintains in designated record sets.

Upon receiving a request from an individual (or from a minor's parent or an individual's personal representative) for disclosure of an individual's PHI, the employees will take the following steps:

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

- Review the disclosure request to determine whether the PHI requested is held in the individual's designated record set. See the Privacy Official if it appears that the requested information is not held in the individual's designated record set. No request for access may be denied without approval from the Privacy Official.
- Review the disclosure request to determine whether an exception to the disclosure requirement might exist; for example, disclosure may be denied for requests to access psychotherapy notes, documents compiled for a legal proceeding, information compiled during research when the individual has agree to denial of access, information obtained under a promise of confidentiality, and other disclosures that are determined by a health care professional to be likely to cause harm. See the Privacy Official if there is any question about whether one of these exceptions applies. No request for access may be denied without approval from the Privacy Official.
- Respond to the request by providing the information or denying the request within 30 days. If the requested PHI cannot be accessed within the 30-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30 -day period of the reasons for the extension and the date by which the Employer will respond.
- A Denial Notice must contain (1) the basis for the denial; (2) a statement of the individual's right to request a review of the denial, if applicable; and (3) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Official.
- Provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual.
- Individuals have the right to receive a copy by mail or by e-mail or can come in and pick up a copy. Individuals (including inmates) also have the right to come in and inspect the information.
- If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, prepare such summary and explanation of the information requested and make it available to the individual in the form or format requested by the individual.
- Charge a reasonable cost-based fee for copying, postage, and preparing a summary (but the fee for a summary must be agreed to in advance by the individual). This provision is not needed if the plan will not charge a fee.

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

Individual's Requests for Amendment

HIPAA also provides individuals the right to request to have their PHI amended. Innermark will consider requests for amendment that are submitted in writing by participants.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for amendment of an individual's PHI held in a designated record set, employees will take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Review the disclosure request to determine whether the PHI at issue is held in the individual's designated record set. See the Privacy Official if it appears that the requested information is not held in the individual's designated record set. No request for amendment may be denied without approval from the Privacy Official.
- Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (see the access procedures above). See the Privacy Official if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Official.
- Review the request for amendment to determine whether the amendment is appropriate—that is, determine whether the information in the designated record set is accurate and complete without the amendment.
- Respond to the request within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Employer will respond.
- When an amendment is accepted, make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the unconnected information to the detriment of the individual.
- When an amendment request is denied, the following procedures apply:
    - All notices of denial must be prepared or approved by the Privacy Official. A Denial Notice must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial.
    - If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement, if any; and the Employer's rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

Request for an Accounting of Disclosures of PHI

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosures, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- If the individual requesting the accounting has already received one accounting within the 12 month period immediately preceding the date of receipt of the current request, prepare a notice to the individual informing

him or her that a fee for processing will be charged and providing the individual with a chance to withdraw the request.
- Respond to the request within 60 days by providing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below). If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Employer will respond.
- The accounting must include disclosures (but not uses) of the requesting individual's PHI made by Plan and any of its business associates during the period requested by the individual up to six years prior to the request. (Note, however, that the plan is not required to account for any disclosures made prior to April 14, 2004. The accounting does not have to include disclosures made:
    - to carry out treatment, payment and health care operations;
    - to the individual about his or her own PHI;
    - incident to an otherwise permitted use or disclosure;
    - pursuant to an individual authorization;
    - for specific national security or intelligence purposes;
    - to correctional institutions or law enforcement when the disclosure was permitted without an authorization; and
    - as part of a limited data set.

- If any business associate of the Plan has the authority to disclose the individual's PHI, then Privacy Officer shall contact business associate to obtain an accounting of the business associate's disclosures.
- The accounting must include the following information for each reportable disclosure of the individual's PHI:
    - the date of disclosure;
    - the name (and if known, the address) of the entity or person to whom the information was disclosed;
    - a brief description of the PHI disclosed; and
    - a brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)

- If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of disclosures of PHI would be reasonably likely to impede the agency's activities, disclosure may not be required. If an employee receives such a statement, either orally or in writing, the employee must contact the Privacy Official for more guidance.
- Accountings must be documented in accordance with the procedure for "Documentation Requirements."

Requests for Confidential Communications

Individuals may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if the requests are reasonable.

However, the Employer shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
- The employee should take steps to honor requests.
- If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

- All confidential communication requests that are approved must be tracked.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

Requests for Restrictions on Uses and Disclosures of PHI

Individuals may request restrictions on the use and disclosure of the participant's PHI. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for access to an individual's PHI, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- The employee should take steps to honor requests.
- If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
- All requests for limitations on use or disclosure of PHI that are approved must be tracked.
- All business associates that may have access to the individual's PHI must be notified of any agreed-to restrictions.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

Records

Copies of all of the following items will be maintained for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

- “Notices of Privacy Practices" that are issued to participants
- Copies of policies and procedures
- Individual authorizations
- When disclosure of certain PHI is made:
    - Date of the disclosure;
    - Name of the entity or person who received the PHI and, if known, the address of such entity or person;
    - Brief description of the PHI disclosed;
    - Brief statement of the purpose of the disclosure; and
    - Any other documentation required under these Use and Disclosure Procedures.

Revision History

Version	Date	Editor	Approver	Description of Changes	Format
1.0	1/1/2026	Tom Robertson	Tom Robertson	Initial	