HIPAA Privacy Use and Disclosure Procedures

Introduction

UnitedAg ("the Company") sponsors and self-administers a group health plan (the Plan). Members of the Company's workforce may have access to protected health information (PHI) of Plan participants (1) on behalf of the Plan itself.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Company's ability to use and disclose PHI. In addition, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and its implementing regulations impose additional requirements-with different effective dates for various provisions.

> *Protected Health Information.* PHI means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. PHI includes information of persons living or deceased. For purposes of these Procedures, PHI does not include the following:
>
> 1. summary health information, as defined by HIPAA's privacy rules, that is disclosed to the Company solely for purposes of (a) obtaining premium bids or (b) modifying, amending, or terminating the Plan;
> 2. enrollment and disenrollment information concerning the Plan that does not include any substantial clinical information;
> 3. PHI disclosed to the Plan or the Company under a signed authorization that meets the requirements of the HIPAA privacy rules;
> 4. PHI for an individual who has been deceased for more than 50 years;
> 5. information used by, or disclosed to, the Company for functions that the Company performs in its role as an employer and not as sponsor of the Plan or in providing administrative services to the Plan.

It is the Company's policy to comply fully with HIPAA's requirements. To that end, all members of the Company's workforce who have access to PHI must comply with these Use and Disclosure Procedures. For purposes of these Use and Disclosure Procedures and the Company's, the Company's workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Company, whether or not they are paid by the Company. The term "workforce member" includes all of these types of workers.

No third-party rights (including but not limited to rights of Plan participants, beneficiaries, covered

dependents, or business associates) are intended to be created by these Use and Disclosure Procedures. The Company reserves the right to amend or change these Use and Disclosure Procedures at any time (and even retroactively) without notice. To the extent these Use and Disclosure Procedures establish requirements and obligations above and beyond those required by HIPAA, these Use and Disclosure Procedures shall be aspirational and shall not be binding upon the Company. To the extent these Procedures are in conflict with the HIPAA privacy rules, the HIPAA privacy rules will govern. These Use and Disclosure Procedures do not address requirements under other federal laws or under state laws.

I. Procedures for Use and Disclosure of PHI

A. Use and Disclosure Defined

The Company and the Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of PHI by any workforce member of the Company, or by a Business Associate of the Plan.
- *Disclosure.* The release, transfer, provision of access to, or divulging in any other manner of PHI to a workforce member who is not a workforce member with access (defined below), or to a person or entity that is not a Business Associate of the Plan.

B. Workforce Must Comply With Company's Policy and Procedures

All members of the Company's workforce must comply with these Use and Disclosure Procedures.

C. Access to PHI Is Limited to Certain Workforce Members

The following workforce members ("workforce members with access") have access to PHI:

- Claims Department personnel
- Customer Service personnel
- Underwriting Department personnel
- Billing/Eligibility personnel
- Accounting/Actuarial personnel; and
- Employees of the Plan Administrator for its use in “plan administrative functions”.

The same workforce members may be named or described in both of these two categories.

These workforce members with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other workforce members with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Workforce members with access may not disclose PHI to other workforce members (other than workforce members with access) except in accordance with these Use and Disclosure Procedures.

D. Permitted Uses and Disclosures of PHI: Payment and Health Care Operations Definitions

Payment. Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's benefit obligations, 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.

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; and
- business management and general administrative activities.

Uses and Disclosures for Plan's Own Payment Activities or Health Care Operations. A workforce member with access may use and disclose PHI to perform the Plan'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. A workforce member with access may disclose PHI to another covered entity or health care provider to perform the other entity's payment activities. Disclosures may be made under the following procedures:

- Disclosures must comply with the "Minimum-Necessary Standard." (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Disclosures for Certain Health Care Operations of the Receiving Entity. A workforce member with access 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 subject to the following:

- The disclosure must be approved by the Privacy Official.
- Disclosures must comply with the "Minimum-Necessary Standard."
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Use or Disclosure for Purposes of Non-Health Benefits. Unless an authorization from the individual (as discussed in "Disclosures Pursuant to an Authorization") has been received, a workforce member may not use PHI for the payment or operations of the Company's "non-health" benefits (e.g., disability, worker's compensation, and life insurance). If a workforce

member requires PHI for the payment or health care operations of non-Plan benefits, follow these steps:

- Obtain an Authorization. First, contact the Privacy Official to determine whether an authorization for this type of use or disclosure is on file. If no form is on file, request an appropriate form from the Privacy Official. ***Workforce members shall not attempt to draft authorization forms. All authorizations for use or disclosure for non-Plan purposes must be on a form provided by (or approved by) the Privacy Official.***
- The disclosure must be approved by the Privacy Official.
- Disclosures must comply with the "Minimum-Necessary Standard."
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Questions? Any workforce member 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.

E. Mandatory Disclosures of PHI: To Individuals and HHS

Request From Individual. Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own PHI to the individual or to a third party identified by the individual, the workforce member must follow the procedure for "Disclosures to Individuals Under Right to Access Own PHI."

Request From HHS. Upon receiving a request from HHS for disclosure of PHI, the workforce member must take the following steps:

- Follow the procedures for verifying the identity of a public official set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

F. Permissive Disclosures of PHI: For Legal and Public Policy Purposes

Disclosures for Legal or Public Policy Purposes. A workforce member who receives a request for disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Disclosures Covered" must contact the Privacy Official. Disclosures may be made under the following procedures:

- The disclosure must be approved by the Privacy Official.
- Disclosures must comply with the "Minimum-Necessary Standard" unless otherwise required by law.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Legal and Public Policy Uses and Disclosures Covered

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 is

necessary to prevent harm to the individual (or other potential victims) or the individual is incapacitated and unable to agree and the information will not be used against the individual and is necessary for an immediate enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk of serious harm or if informing the individual would involve a personal representative who is believed to be responsible for the abuse, neglect, or violence and informing that person would not be in the best interest of the individual, as determined by the Privacy Official in the exercise of professional judgment..

Judicial and Administrative Proceedings, in response to:

- An order of a court or administrative tribunal (provided that disclosure must be limited to PHI expressly authorized by the order); and
- A subpoena, discovery request or other lawful process, not accompanied by the order of a court 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 obtain a qualified protective order.

Law-Enforcement Official for Law-Enforcement Purposes, under the following conditions:

- Pursuant to a legal process and as otherwise required by law, but only if the information sought is relevant and material to a legitimate law-enforcement inquiry, the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and de-identified information could not reasonably be used.
- Information requested is limited information to identify or locate a suspect, fugitive, material witness, or missing person.
- Information about an individual who is a victim or 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, is needed to determine whether a violation of law occurred, the need for the information is urgent, and disclosure is in the best interest of the individual as determined by the Privacy Official in the exercise of professional judgment.
- Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.
- Information that constitutes evidence of criminal conduct that occurred on the Company's premises.

Appropriate Public Health Authorities for Public Health Activities.

Health Oversight Agency for Health Oversight Activities, as authorized by law.

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.

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.

Certain Limited-Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.

Avert a Serious Threat to Health or Safety, upon a good faith belief 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, and the use or disclosure is to a person reasonably able to prevent or lessen the threat, including to the target of the threat.

Specialized Government Functions, including disclosures of an inmate's PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials for the conduct of national security activities.

Workers' Compensation Programs, to the extent necessary to comply with laws relating to workers' compensation or other similar programs providing benefits in case of occupational illness or injury.

G. Disclosures of PHI Pursuant to an Authorization Procedure

Disclosure Pursuant to Individual Authorization. Any requested disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required under these Use and Disclosure Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

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

Verify that the authorization form is valid and has not expired or been revoked. Valid authorization forms are those that:

- Contain a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- Identify the person (or class of persons) authorized to make the requested use or disclosure;
- Identify the person (or class of persons) to whom the Plan may make the use or disclosure;
- Contain a description of each purpose of the use or disclosure (statement that the use or disclosure is made "at the request of the individual" is sufficient if the individual initiates the authorization and does not provide a specific purpose);
- Contain an expiration date or an expiration event (e.g., when coverage ends) that relates to the individual or the purpose of the use or disclosure;
- Contain a statement regarding the individual's right to revoke the authorization, the procedures for revoking authorizations, and any exceptions to the right to revoke;
- Contain a statement regarding the possibility for a subsequent redisclosure of the information;
- Contain a statement of the ability or inability of the Plan to condition payment, enrollment, or eligibility on submission of the authorization; and
- Contain the signature of the individual and the date signed; if the authorization is signed by a personal representative of the individual, it must include a description of the

representative's authority to act for the individual.

- All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

H. Disclosure of PHI to Business Associates

Business Associate is an entity or person who:

- creates, receives, maintains, or transmits PHI on behalf of the Plan (including for claims processing, or administration, data analysis, or underwriting); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services to or for the Plan, where the service provider has access to PHI.

Use and Disclosure of PHI by Business Associate. All uses and disclosures by a "business associate" must be made in accordance with applicable law and a valid business associate contract. Before allowing a business associate to create, receive, maintain, or transmit PHI on behalf of the Plan, workforce members 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 applicable law and 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 nonrecurring disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

I. Requests From Spouses, Family Members, and Friends for Disclosure of PHI

The Plan and the Company will not disclose PHI to family and friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member, or friend, will be able to access PHI.

If a workforce member receives a request for disclosure of an individual's PHI from a spouse, family member, or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information."

Once the identity of a parent or personal representative is verified, then follow the procedure for "Request for Individual Access."

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."

J. Disclosures of De-Identified Information

De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

*Procedure***.** Obtain approval from Privacy Official for the disclosure. The Privacy Official will verify that the information is de-identified.

The Plan may freely use and disclose de-identified information. De-identified information is not PHI.

K. Verification of Identity of Those Requesting Protected Health Information

Verifying Identity and Authority of Requesting Party. Workforce members with access 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. Workforce members 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 there is any doubt as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, the workforce member should 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, confirm the social security number of the individual.
- 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. 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 obtain other evidence or documentation of authority, 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 Privacy Official.
- Obtain approval for the disclosure from the Privacy Official.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

L. Complying With the "Minimum-Necessary" Standard

Procedures for Disclosures. 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. For all other requests for PHI, contact the Privacy Official, who will ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Exceptions. The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made for treatment of the individual;
- 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.

M. Documentation

Documentation. Workforce members shall maintain copies of all of the following items 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:
  - the date of the disclosure;
  - the name of the entity or person who received the PHI and, if known, the address of such entity or person;
  - a brief description of the PHI disclosed;
  - a brief statement of the purpose of the disclosure; and
  - any other documentation required under these Use and Disclosure Procedures.

Note: The retention requirement only applies to documentation required by HIPAA. It does not apply to all medical records.

N. Mitigation of Inadvertent Disclosures of PHI

Mitigation: Reporting Required. HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to the Plan of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this manual. As a result, anyone who becomes aware of a disclosure of PHI, whether by a workforce member, a Business Associate, or other outside consultant/contractor, that is not in compliance with the policies and procedures set forth in this manual, should immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the individual can be taken.

O. Breach Notification Requirements

Compliance. The Plan will comply with the final regulations at 45 CFR §164.400 et seq. for breaches of unsecured PHI that occur on or after September 23, 2013 and will comply with the requirements of the interim final regulations for breaches of unsecured PHI that occur on or after September 23, 2009 and before September 23, 2013. The procedures for such notifications are set forth in Appendix B to the Privacy Policy ("Reportable Breach Notification Policy").

II. Procedures for Complying With Individual Rights

A. Individual's Request for Access

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

- the 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.

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or from a minor's parent or an individual's personal representative) for disclosure of an individual's PHI to the individual or to a third party, the workforce member must take the following steps:

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

- Review the disclosure request to determine whether the PHI requested is held in one or more designated record sets. See the Privacy Official if it appears that the requested information is not held in any 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, certain requests by inmates, information compiled for research purposes if the individual has agreed 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, explaining the reasons for the extension and the date by which the Company 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 a readable hard copy form. Individuals (except for inmates) have the right to receive a copy by mail or by email, 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 PHI requested is maintained electronically in one or more designated record sets, and the individual requests an electronic copy of such information, the Plan will provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; if the PHI is not readily producible in such form and format, the PHI will be produced in a readable electronic form and format as agreed by the Plan and the individual. If the Plan and the individual cannot agree on an acceptable electronic form and format, the Plan will provide a paper copy of 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.

Plan shall charge a fee of $0.25 per page or a maximum of $25.00 for copying and postage of requested PHI. If the individual requests a summary and explanation of the information requested, Plan shall charge $10.00 for each hour necessary for the preparation of such information.

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

B. Individual's Request for Amendment

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for amendment of an individual's PHI held in a designated record set, the workforce member must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Review the amendment 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 Company will respond.
- When an amendment is accepted, make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.
- When an amendment request is denied, the following procedures apply:
    - All notices of denial must be prepared or approved by the Privacy Official. A Denial Notice must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial.
    - 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 Company'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.

C. Processing Requests for an Accounting of Disclosures of Protected Health Information

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosures, the workforce member 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 or revise 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 Company will respond.
- The accounting must include disclosures (but not uses) of the requesting individual's PHI made by the Plan and any of its business associates during the period requested by the individual up to six years prior to the request. The accounting does not have to include disclosures made:
    - to carry out treatment, payment, and health care operations;
    - to the individual about his or her own PHI;
    - incident to an otherwise permitted use or disclosure;
    - pursuant to an individual authorization;
    - to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
    - for specific national security or intelligence purposes;
    - to correctional institutions or law enforcement when the disclosure was permitted without an authorization; and
    - as part of a limited data set.

If any business associate of the Plan has the authority to disclose the individual's PHI, then the employee must contact the business associate to obtain an accounting of the business associates disclosures.

The accounting must include the following information for each disclosure of the individual's PHI:

- the date of disclosure;
- the name (and, if known, the address) of the entity or person to whom the information was disclosed;
- a brief description of the PHI disclosed; and
- a brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)

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

Accountings must be documented in accordance with the procedure for "Documentation Requirements."

D. Processing Requests for Confidential Communications

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the workforce member 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 workforce member should take steps to honor requests that are reasonable in motivation and rationale or if failure to disclose could endanger the individual.
- If a request will not be accommodated, the workforce member 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 recorded in the Benefits Inquiry system.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

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

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for a restriction on the use and/or disclosure of the individual's PHI, the workforce member 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 workforce member should take steps to honor requests, however requests for restrictions on use and disclosure are not required to be honored by the Plan, but the Plan may wish to honor reasonable requests. Refer to the request Privacy Official.
- The Plan will comply with a restriction request if (1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment), and (2) the PHI pertains solely to a health care item or service for which the health care provider has been paid in

full by the individual or another person, other than the Plan.

- If a request will not be accommodated, the workforce member must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
- All requests for restrictions on use or disclosure of PHI that are approved must be tracked on the Plan benefits inquiry system.
- All business associates that may have access to the individual's PHI must be notified in writing of any agreed-to restrictions.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."