Arthur J. Gallagher & Co. (Illinois)
Employees' Self-Funded Medical/Dental Plan
And Insured Benefits
Including Severance Plan, Insured Basic Life and AD&D, Long Term Disability, Business Travel Accident, Voluntary AD&D, Voluntary Vision, Wellbeing Program, Flexible Spending and Resources for Work and Life/Employee Assistance Plan

HIPAA Privacy and Security Policy

Effective April 14, 2003

(Revised September 2019)

Gallagher

Insurance | Risk Management | Consulting

Table of Contents

HIPAA Privacy Policy
Introduction

Arthur J. Gallagher & Co. (Illinois) ("the Company") sponsors group health (including a wellbeing program), dental, vision, flexible spending, and resources for work and life/employee assistance plan ("the Plans"). Members of the Company's workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plans themselves; or (2) on behalf of the Company, for administrative functions of the Plans.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Company's ability to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Plans 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 for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

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 this Privacy Policy. For purposes of this Policy, 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 "employee" includes all of these types of workers.

The Plans will not use PHI that is genetic information for underwriting purposes. Uses and disclosures of psychotherapy notes will be made only with authorization from you.

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 this Policy. The Company reserves the right to amend or change this Policy at any time (and even retroactively) without notice. This Policy does not address requirements under other federal laws or under state laws.

Plans' Responsibilities as Covered Entities

1. Privacy Official and Contact Person

The Company's Corporate Director of U.S. Benefits is the Privacy Official of U.S. Benefit Plans. The Privacy Official of U.S. Benefit Plans is responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to, this Privacy Policy and the Company's use and disclosure procedures. The Privacy Official also serves as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI.

2. Workforce Training

It is the Company's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. The Privacy Official of U.S. Benefit Plans is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions within the Plans.

3. Technical and Physical Safeguards and Firewall

The Company has established on behalf of the Plans appropriate technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets.

Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for plan administrative functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

4. Privacy Notice

The Privacy Official of U.S. Benefit Plans is responsible for developing and maintaining a notice of the Plans' privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Plans;
- the individual's rights; and
- the Plans' legal duties with respect to the PHI.

The privacy notice informs participants that the Company will have access to PHI in connection with its plans' administrative functions. The privacy notice also provides a description of the Company's complaint procedures, the telephone number of the Privacy Official for further information and the date of the notice.

The notice of privacy practices will be individually delivered to all participants:

- at the time of an individual's enrollment in the Plans,
- on an ongoing basis, and
- within 60 days after a material change to the notice.

The Plans will also provide notice of availability of the privacy notice at least once every three years.

5. Complaints and Violations

The Privacy Official of U.S. Benefit Plans is responsible for the process that individuals use to report complaints and violations about the Plans' privacy procedures and for the system used to handle such reports. A copy of the complaint procedure shall be provided to any participant upon request.

The Privacy Official below is Plans' contact person for receiving complaints and reports of violations:

Privacy Official of U.S. Benefit Plans
Arthur J. Gallagher & Co. (Illinois)
Human Resources
2850 Golf Road
Rolling Meadows, IL 60008
Phone: 630-773-3800
Fax: 630-773-4000

6. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed, up to and including termination of employment. Inadvertent use or disclosure of PHI will be subject to a verbal or written warning. Blatant and purposeful use or disclosure without regard for this privacy policy will be subject to termination of employment.

7. Mitigation of Inadvertent Disclosures of Protected Health Information

The Company shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this Policy. As a result, if an employee becomes aware of a use or disclosure of protected health information, either by an employee of the Plans or an outside consultant/contractor, that is not in compliance with this Policy, the employee is required to immediately contact the Privacy Official of U.S. Benefit Plans so that the appropriate steps to mitigate the harm to the participant can be taken.

8. No Intimidating or Retaliatory Acts – No Waiver of HIPAA Privacy

No employee of the Company may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

9. Plan Documents

The Plans' documents include provisions describing the permitted and required uses and disclosures of PHI by the Company for plan administrative purposes. Specifically, the Plans' documents require the Company to:

- not use or further disclose PHI other than as permitted by the Plans or as required by law;
- ensure that any agents or subcontractors to whom it provides PHI received from the Plans agree to the same restrictions and conditions that apply to the Company;
- not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan;
- report to the Privacy Official of U.S. Benefit Plans any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures as required by law;
- make the Company's internal practices and records relating to the use and disclosure of PHI received from the Plans available to the Department of Health and Human Services (DHHS) upon request; and
- if feasible, return or destroy all PHI received from the Plans that the Company still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

The Plans' documents also require the Company to (1) certify to the Privacy Official of U.S. Benefit Plans that the Plans' documents have been amended to include the above restrictions and that the Company agrees to those restrictions, and (2) provide adequate safeguards.

10. Documentation

The Plans' and the Company's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as

necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

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

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. The Company must maintain such documentation for at least six years.

Documentation Requirements. Plans 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.
- When a disclosure of 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.
- Individual authorizations.

Policies and Procedures on Use and Disclosure of PHI

1. Use and Disclosure Defined

The Company and the Plans 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 individually identifiable health information by any person working for or within the Company or by a Business Associate (defined below) of the Plan.

Disclosure. For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons within the Company who would not otherwise have access and persons not employed by or working within the Company.

2. 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.

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 a valid authorization;
- disclosures made to the DOL;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

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

All members of the Company's workforce (described in the Introduction of this Policy and referred to herein as "employees") must comply with this Policy and with the Company's use and disclosure procedures, which are set forth in this document.

4. Access to PHI Is Limited to Certain Employees

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

- employees of the Company’s Human Resource, Finance, Audit and Legal departments, members of the Benefits Committee, employees of the Company’s Benefits Consulting and Administration divisions who perform

functions directly on behalf of the Plans or who have access to PHI on behalf of the Company for its use in the Plans' administrative functions.

These employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (subject to the minimum necessary standard). 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 Procedures document.

5. Permitted Uses and Disclosures – Payment and Health Care Operations

Payment. Payment includes activities undertaken to obtain the Plans' contributions or to determine or fulfill the Plans' responsibilities for provision of benefits under the Plans, or to obtain or provide reimbursement for health care. Payment includes but is not limited to:

- eligibility and coverage determinations including coordination of benefits and adjudication (e.g. claim administration) 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.

PHI, subject to the minimum necessary, may be disclosed for the Plans' own payment purposes and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

Health Care Operations. Health care operations means any of the following activities, but not limited to, to the extent that they are related to the Plans' 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.

PHI, subject to the minimum necessary, may be disclosed for purposes of the Plans' own 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.

6. No Disclosure of PHI for Non-Health Plan Operations

PHI may not be used or disclosed for the payment or operations of the Company's "non-health" benefits (e.g., disability, 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. Disclosures must be the minimum necessary, and be approved and documented by the Privacy Official.

In certain circumstances PHI may be disclosed for purposes of administering the Company's workers' compensation plan. In these cases, the Company will direct the workers' compensation plan to request the disclosure of the PHI directly from the organization holding original data.

7. Mandatory Disclosures of PHI to the Individual and DHHS

A participant's PHI must be disclosed as required by HIPAA in two situations:

- 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"); or
- the disclosure is made to DHHS for purposes of enforcing of HIPAA.

8. Permissive Disclosures of PHI for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization when the specified requirements are satisfied. The disclosures must be the minimum necessary and be approved and documented by the Privacy Official of U.S. Benefit Plans. Permitted disclosures in this category are:

A. About victims of abuse, neglect or domestic violence if:

- 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; or
- the individual agrees with the disclosure.

B. For judicial and administrative proceedings if:

- 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.

C. For law enforcement purposes if:

- 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, or
- information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person, or
- 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, or
- information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct, or
- information that constitutes evidence of criminal conduct that occurred on the Company's premises.

D. For public health activities and health oversight activities.

E. About decedents if:

- for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by laws.

F. For cadaveric organ, eye or tissue donation purposes if:

- 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.

G. For certain limited research purposes:

- provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.

H. To avert a serious threat to health or safety if:

- 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.

I. For specialized government functions if:

- 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.

J. That relate to workers' compensation programs if:

- only to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

9. Disclosures of PHI Pursuant to an 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 the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

10. Complying With the "Minimum Necessary" Standard

Minimum Necessary When Disclosing PHI. For making *routine and recurring disclosures* of PHI the following applies:

Disclosures	Recipient(s)	Company Policy
Marketing	Consultant Insurance carriers Providers TPAs	Provide summary and de-identified information. Provide PHI at final negotiation, if required.
Claim Issue Resolution	TPAs Providers Insurance carriers Consultants Appeals Committee Legal counsel	Direct participant to TPA, insurance carrier or plan provider. Disclose minimum necessary when seeking professional opinions or presenting an appeal.
Billing Issue Resolution	TPAs Insurance carriers Providers Consultants Payroll and Finance departments	Disclose minimum necessary PHI to resolve issue. Obtain participant authorization if necessary.
Compliance Issue Resolution	TPAs Insurance carriers Providers Consultants Legal counsel	Provide minimum PHI necessary to secure legal opinion.

All other disclosures must be reviewed on an individual basis with the Privacy Official of U.S. Benefit Plans to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. For making *routine and recurring requests* for disclosure of PHI the following applies:

Requests	Recipient(s)	Company Policy
Health Plan Marketing	Health plan TPA Insurance carrier	Request Summary and De-identified information and PHI only if required
Renewal Underwriting and Experience Evaluation	Health plan TPA Insurance carrier	Request Summary and De-identified information and PHI only if required
Claims Audit	Health plan TPA Insurance carrier	Request Summary and De-identified information and PHI only if required
Claim Issue Resolution	Health plan TPA Insurance carrier	Request Summary and De-identified information and PHI only if required
Billing Issue Resolution	Health plan TPA Insurance carrier	Request Summary and De-identified information and PHI only if required
Compliance Issue Resolution	Health plan TPA Insurance carrier Individual Outside legal	Request Summary and De-identified information and PHI only if required
COBRA Rate or Funding Level Determination	Health plan TPA Insurance carrier	Request Summary and De-identified information and PHI only if required
Network Discount Evaluation	Health plan TPA Insurance carrier	Request Summary and De-identified information and PHI only if required
Disruption Analysis	Health plan TPA Insurance carrier	Request Summary and De-identified information and PHI only if required
Strategic Planning	Health plan TPA Insurance carrier	Request Summary and De-identified information and PHI only if required

All other requests must be reviewed on an individual basis with the Privacy Official of U.S. Benefit Plans to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

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 DHHS;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

11. Disclosures of PHI to Business Associates

Employees with access may disclose PHI to the Plans' business associates and allow the Plans' business associates to create or receive PHI on its behalf. However, prior to doing so, the Plans must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees with access must contact the Privacy Official of U.S. Benefit Plans and verify that a business associate contract is in place.

Business Associate. A business associate is an entity that:

- performs or assists in performing the Plans' function or activities 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.

12. Disclosures of De-identified Information

The Plans may freely use and disclose 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 the Company can determine that information is de-identified, either (1) by professional statistical analysis, or (2) by removing 18 specific identifiers. These identifiers are:

- names
- all geographic subdivisions smaller than State (special rules apply)
- all elements of dates (except year) relating directly to an individual (special rules apply)
- telephone numbers
- fax numbers
- electronic mail addresses
- Social Security numbers
- medical record numbers
- health plan beneficiary numbers
- account numbers
- certificate/license numbers
- vehicle identification and serial numbers including license plate numbers
- device identifiers and serial numbers
- web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- biometric identifiers including finger and voice prints
- full face photographic images and any comparable images
- any other unique identifying number, characteristic or code (special rules apply).

Policies and Procedures on Individual Rights

1. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Plans (or their business associates) maintain in "designated record sets". HIPAA also provides that participants may request to have their PHI amended. The Plans will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

Designated Record Set. A 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 Plans, or
- other PHI used, in whole or in part, by or for the Plans to make coverage decisions about an individual.

Upon receiving a request from a participant (or from a minor's parent or a participant's personal representative) for disclosure of a participant's PHI, the employee must take the following steps:

- Follow the procedures for verifying the identity of the participant (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 participant's designated record set. See the Privacy Official of U.S. Benefit Plans if it appears that the requested information is not held in the participant's designated record set. ***No request for access may be denied without approval from the Privacy Official of U.S. Benefit Plans.***
- 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 during research when the participant 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 of U.S. Benefit Plans 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 (60 days if the information is maintained off-site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days by providing written notice to the

participant within the original 30- or 60-day period of 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 participant's right to request a review of the denial, if applicable, and (3) a statement of how the participant may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Official of U.S. Benefit Plans.
- Provide the information requested in the form or format requested by the participant, 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 participant.
- Participants have the right to receive a copy by mail or by e-mail or can come in and pick up a copy. Participants also have the right to come in and inspect the information.
- Participants have the right to request that the PHI is sent directly to another designated person. This request must be made in writing and signed by the participant. The request must clearly identify the recipient and where the information is to be sent.
- If the participant 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, if feasible, make it available to the participant in the form or format requested by the participant.
- Notify the participant in advance of producing the requested summary that there is a $15 charge copying, postage, and preparing a summary in either a paper or electronic copy. Making up this total fee is a $5 charge for the labor associated with copying the PHI; $5 for copying supplies in either paper or electronic form and $5 for postage.
- Disclosures must be documented in accordance with the procedure "Documentation Requirements."

Implementation Specifications of Requests for Amendment. If a participant submits a written request to amend any PHI maintained in the designated record set, the covered entity will respond to or act upon the request in a timely manner but no later than 60 days after the receipt of the request. The covered entity will respond to the request in one of the following ways:

- Notify the participant that the request for amendment is granted, either in whole or in part. The participant will need to verify their identity and agree to have covered entity notify all relevant parties of the amendment. The covered entity will then make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and attaching the amendment to the record.
- Notify the participant that request for amendment is denied, either in whole or in part, the covered entity will provide the participant with the basis for the denial in writing.

- If the covered entity cannot take action on the request within 60 days of receipt, the time period for action may be extended for 30 days as long as the participant is notified in writing of the reasons for the delay and the date that the request will be acted upon. The covered entity may only have one such extension.

2. Verification of Identity of Those Requesting Protected Health Information

Verifying Identity and Authority of Requesting Party. The Plans must take steps to verify the identity of participants 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 participant, 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 Participant. When an participant requests access to his or her own PHI, the following steps should be followed:

- Request a form of identification from the participant or authorized representative. The Plans will confirm the participant's personal data such as birth date and/or Social Security Number. A participant's request via email on the Company intranet will also serve to verify a participant's identification.
- Verify that the identification matches the identity of the participant or authorized representatives 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 of U.S. Benefit Plans.
- If identification is provided in paper form, the Plans will file it with the relevant participant file maintained by the Company or the third party administrator.
- If the participant or authorized representative requests PHI over the telephone, the Plans will require confirmation of the participant's Social Security Number and date of birth.
- 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 by verifying personal data maintained in the Company's Human Resource Information System such as child's birth date and/or Social Security Number.
- Disclosures must be documented in accordance with the procedure "Documentation Requirements."

Request Made by Personal Representative. When a personal representative requests access to an participant's PHI, the following steps should be followed:

- Require a copy of appropriate documentation such as a valid power of attorney or other documentation deemed valid by state-by-state. If there are any questions about the validity of this document, seek review by the Privacy Official of U.S. Benefit Plans.
- Make a copy of the documentation provided and file it with the relevant participant file maintained by the Company or third party administrator.
- 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 relevant participant file maintained by the Company or third party administrator.
- 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 Company’s Legal Department.
- Obtain approval for the disclosure from the Privacy Official of U.S. Benefit Plans.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

3. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
- as part of a limited data set; or
- for other national security or law enforcement purposes.

The Plans shall respond to an accounting request within 60 days. If the Plans are unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party**,** a brief description of the information disclosed and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Privacy Official of U.S. Benefit Plans may impose reasonable production and mailing costs for subsequent accountings.

Request From Participant, Parent of Minor Child or Personal Representative. Upon receiving a request from a participant (or a minor's parent or a participant's personal representative) for an accounting of disclosures, the employee must take the following steps:

- Follow the procedures for verifying the identity of the participant (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- If the participant 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 participant informing him or her that a $15 fee for processing will be charged and provide the participant 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 participant 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 participant within the original 60-day period of the reasons for the extension and the date by which the Plans will respond.
- The accounting must include disclosures (but not uses) of the requesting individual's PHI made by the Plans and any of their 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 participant 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 participant's PHI, then provide the participant with the contact information for that particular business associate, for example, the Plan's claims payer. The accounting must include the date for each reportable disclosure of the individual's PHI.

4. Requests for Alternative Communication Means or Locations

Participants 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, in the sole discretion of the Company, the requests are reasonable.

However, the Company 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 of U.S. Benefit Plans has responsibility for administering requests for confidential communications.

Request From Participant, Parent of Minor Child or Personal Representative. Upon receiving a request from a participant (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:

- Follow the procedures for verifying the identity of the participant (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 participant.
- The employee should take steps to honor requests that are reasonable based on the facts and circumstances of a given situation and can be verified through other sources (applicable written documentation or employment records).
- If a request will not be accommodated, the employee must contact the participant in person, in writing or by telephone to explain why the request cannot be accommodated.

- All confidential communication requests that are approved must will be initiated by receiving party (the Plans, the Company, one of the Plans' business associates) and provided as soon as possible to the most reasonable party to implement the request.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

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

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the Company's policy to attempt to honor such requests if, in the sole discretion of the Company, the requests are reasonable. The Privacy Official of U.S. Benefit Plans is charged with responsibility for administering requests for restrictions.

Request From Participant, Parent of Minor Child or Personal Representative. Upon receiving a request from an individual (or a minor's parent or a participant's personal representative) to restrict access to an individual's PHI, the employee must take the following steps:

- Follow the procedures for verifying the identity of the participant (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 that are reasonable given the facts and circumstances surrounding the request.
- If a request will not be accommodated, the employee must contact the participant 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 implemented by the most practical party to enforce such request and remain in inforce until the participant has withdrawn the request or circumstances no long make the request a valid request.
- All business associates that may have access to the participant's PHI must be notified of any agreed-to restrictions by the most appropriate representative of the Plans (or the party that first initiates the implementation of the restriction).
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

The Plan will agree to the request if the disclosure is for the purposes of carrying out payment of health care operation and is not otherwise required by law, and the PHI pertains solely to a health care item or service for which the individuals, or person on behalf of the individual other than the health plan, has paid the covered entity in full.

Policy and Procedures on Policy Violation

1. Notification of Privacy Official of U.S. Benefit Plans

Any employee of the Company or participant in any of the Plans who believes that a violation of the HIPAA Privacy and Security Policy has occurred is required to contact the Privacy Official of U.S. Benefit Plans immediately. In a confidential manner, the Privacy Official of U.S. Benefit Plans will investigate the facts and circumstances of the alleged violation and determine an appropriate course of action.

- Any employee and/or participant who believes that a violation of the HIPAA Privacy and Security Policy has occurred is required to contact the Privacy Official of U.S. Benefit Plans immediately to report the incident in question. The Report of Violation form should be used to document and report a suspected violation. The Report of Violation form will be provided by the Privacy Official of U.S. Benefit Plans when the incident is reported.
- The Privacy Official of U.S. Benefit Plans will investigate the facts and circumstances of the alleged violation and determine an appropriate course of action.

2. Violation Resolution

If it is determined that a violation of the HIPAA Privacy and Security Policy has occurred, all involved parties such as the participants(s), other covered entity, business associate and third party service provider will be notified in a timely manner but in no event not longer than 60 calendar days from the date that the breach incident becomes known. The following will be included in the notification:

- date of breach, date breach discovered and description of what happened;
- description of type of PHI involved;
- description of steps the individual should take to protect him or herself;
- brief description of what is being done to prevent this type of breach from happening again; and
- contact procedures if there are any questions.

In the event that a business associate has committed the breach, the authority may be given to the business associate to determine who is in the best position to notify the involved parties of the breach. The responsibility may be given to the Privacy Official of U.S. Benefit Plans, Plan or business associate.

The resolution of any such violation will seek to restore the level of privacy and security that is required under this Policy. Any deficiency in the HIPAA Privacy and Security Policy or related procedures that contributed to the violation will be

corrected. If monetary damages are found to be due any involved party, then the issue will be settled under the laws of the state of Illinois.

The employee(s) responsible for the violation will be dealt with according to the terms of the Company discipline policy. Depending on the severity of the violation and whether or not is was a blatant violation, disciplinary action may range from verbal warning, written warning and probation, up to and including termination of employment.

If a violation is found to have occurred due to the actions of a third party, appropriate action will be taken to correct the situation and reevaluate the third party relationship with the Plan(s) up to and including termination of the relationship as provided for in the contract or confidentiality or business associate agreement.

- The Privacy Official of U.S. Benefit Plans will notify all involved parties, such as participant(s), other covered entity, and third party service provider, in a timely manner once it has been determined that a violation of the HIPAA Privacy and Security Policy has occurred.
- The resolution of any such violation will seek to restore the level of privacy and security that is required under this Policy.
- The Privacy Official of U.S. Benefit Plans will correct any deficiency in the HIPAA Privacy and Security Policy or related procedures that contributed to the violation.
- Monetary damages, if due any involved party, will be settled under the laws of the state of Illinois.
- Employee(s) found responsible for the violation will be subject to the terms of the Company discipline policy. Disciplinary action may range from verbal warning, written warning and probation, up to and including termination of employment. The Privacy Official of U.S. Benefit Plans, Company management and Human Resources will make this determination.
- If a violation is found to have occurred due to the actions of a third party service provider, the Privacy Official of U.S. Benefit Plans and the Company will take appropriate action up to and including terminating service provider's relationship with the Plans.

3. Violation Tracking

The Privacy Official of U.S. Benefit Plans will track all reported incidents of potential violation under this policy whether or not a reported incident is ultimately found to be an actual violation. Tracking includes maintaining the relevant facts of a reported incident and the final determination or resolution.