Privacy and Security Policy
(Including HIPAA)

EFFECTIVE April 20, 2003

Revised June 1, 2020

Privacy and Security Policy
(Including HIPAA)

Introduction

Gallagher Benefit Services, Inc. along with its benefits consulting affiliates (collectively "Gallagher"), by virtue of the services that it performs for its clients' health plans and certain insurance carriers is a "business associate," as that term is defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) under the Administrative Simplification Subtitle at 45 CRF § 160.103. The specific health plans and insurance carriers are "covered entities" as that term is defined by HIPAA.

Gallagher handles Personally Identifiable Information (PII) of its clients as that term is defined herein. Gallagher undertakes to protect the privacy and security of such PII as required by applicable state, federal and international laws and regulations.

In accordance with 1) this Privacy and Security Policy, 2) the current Gallagher Global IT Policies and Standards Manual (GITPSM), (see link below), 3) the Gallagher Benefit Services (GBS) Privacy and Security Procedures (HIPAA-PHI and PII), and Gallagher's Business Operating Standards and Systems (BOSS), Gallagher agrees to undertake certain responsibilities as required by HIPAA regulations.

Link to GITPSM: https://go.ajgco.com/apps/itpolicy/SitePages/Home.aspx

Plans Subject to this Policy

The following health plans are affected and must comply with HIPAA regulations, as well as laws regulating the protection of PII: medical, dental, vision, hearing, prescription drug, health care flexible spending account, some employee assistance programs and long term care.

The following plans are *not* covered under HIPAA: life, disability, and workers compensation. However, information relating to these plans may still need to be safeguarded as per the terms of this Policy because it would be considered PII.

Business Associate Agreements (HIPAA Specific Requirement)

Gallagher enters into business associate agreements with covered entities that permit Gallagher to use and disclose protected health information (PHI) belonging to the covered entity. As such, Gallagher has specific obligations as a Business Associate under HIPAA and this Policy addresses those obligations. While all Gallagher employees are expected to be familiar with and follow our business associate agreements with covered entities, it is the responsibility of the most senior account person on a client team to ensure that the terms are carried out in daily operations and guide the use of protected data.

Protected Health Information (HIPAA)

HIPAA and its implementing regulations restrict Gallagher's ability to use and disclose PHI.

Protected Health Information (PHI) means information that is:

1. *created or received by a covered entity, and*
2. *relates to the past, present, or future physical or mental health or condition of an individual or the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and*

    a. *that identifies the individual, or*
    b. *there is a reasonable basis to believe the information can be used to identify the individual.*

Protected health information includes information of persons living or deceased.

For purposes of this Policy, PHI is defined as personal health information that is related to any covered health plan. Enrollment data that is comprised of both census data and coverage data is considered PHI. Census data alone is not PHI as long as it does not include enrollment data. PHI also includes claims detail such as large claim reports, monthly claim reports, copies of EOBs, etc., and information used for utilization review management, disease management and wellness programs. Electronic PHI (ePHI) is a subset of PHI that encompasses any PHI stored or transmitted in an electronic format. Note that ePHI is included in the definition of PHI as used throughout this Policy.

Generally speaking, Gallagher will not be the sole repository of any form of PHI since Gallagher does not generate PHI as part of its normal business operations. PHI is generated by health plans, providers, health insurance companies and healthcare clearing houses. To the extent that Gallagher is the sole holder of original PHI, then this Policy addresses the relevant HIPAA requirements. To the extent that HIPAA is applicable to the clients Gallagher serves as a Business Associate, this Policy addresses both the needs of those clients (as defined in the terms of the applicable Business Associate Agreement) and the legal requirements of HIPAA.

Personally Identifiable Information

Various state, federal and international laws and regulations restrict Gallagher's ability to use and disclose PII belonging to its clients.

Personally Identifiable Information (PII) means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information:

1. *that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or*
2. *by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a*

combination of gender, race, birth date, geographic indicator, and other descriptors).

Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

Gallagher Workforce

Members of the Gallagher workforce may have access to the individually identifiable information of health plan participants (including PHI and PII) (1) on behalf of a plan itself, (2) on behalf of a plan sponsor, or (3) on behalf of insurance carriers who underwrite a health plan.

It is Gallagher's policy to comply fully with HIPAA's requirements with regard to PHI, as well as other legal requirements applicable to PII. To that end, all members of the Gallagher workforce who have access to PHI/PII must comply with this Policy. For purposes of this Policy, the Gallagher 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 Gallagher, whether or not they are paid by Gallagher. The term "employee" includes all of these types of workers.

No third party rights (including but not limited to rights of health plan participants, beneficiaries, covered dependents, covered entities or other business associates) are intended to be created by this Policy. Gallagher reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA or any applicable law governing the privacy and security of PII, the Policy shall be binding upon Gallagher.

Gallagher Responsibilities

Privacy Officer and Contact Person

Jennifer Ryder is the Privacy Officer for Gallagher. The Privacy Officer is responsible for the development and implementation of policies and procedures relating to privacy including, but not limited to, this Policy and Gallagher's use and disclosure procedures described in the GITPSM. (see link below). The Privacy Officer also serves as the contact person for members of the Gallagher workforce who have questions, concerns or complaints about the privacy of PHI/PII.

Link to GITPSM: https://go.ajgco.com/apps/itpolicy/SitePages/Home.aspx

Security Officer and Contact Person

James Downing is the Security Officer for Gallagher. The Security Officer is responsible for the development and implementation of policies and procedures relating to security management of PHI/PII including, but not limited to, this Policy and Gallagher's data safeguards and information control disclosure procedures described in the GITPSM. The Security Officer also serves as the

contact person for members of the Gallagher workforce who have questions, concerns or complaints about the security of PHI/PII.

Compliance Audit and Oversight Team

The Compliance Audit team in conjunction with IT Compliance will review the information assets (technical and non-technical) on a regular and continuous schedule to evaluate the effectiveness of their controls over PHI/PII and determine if those controls are providing a reasonable and appropriate minimization of risk to Gallagher, its partners and clients, and to the individuals who own the information. The Compliance Audit team will report its findings on a regular basis to the Privacy Officer and to the managers who are responsible for the security and operations of information assets that were assessed.

Workforce Training

It is Gallagher's policy to train all members of its workforce who have access to PHI/PII on its Privacy and Security Policy and related procedures. The Privacy Officer is charged with developing training schedules and programs to ensure that all workforce members receive the training necessary and appropriate to empower them to follow the Gallagher Privacy and Security Policy and related procedures as they carry out their daily functions and work activities under Gallagher's business operations.

Using the AJG Privacy Awareness and AJG Cyber Security Awareness Training Modules, Gallagher will conduct annual privacy and security training for all employees. New hire training is required to be completed within 45 days of assignment. Training is mandatory and each employee is required to electronically sign an acknowledgement certifying they have attended the training and understand their responsibilities. Branch Managers and other managers are responsible for verifying all employees complete these training modules within 45 days of assignment.

Link to AJG Privacy Awareness and AJG Cyber Security Awareness Training:

Privacy: https://gallagher.csod.com/ui/lms-learning-details/app/curriculum/40028abe-c42e-4a1d-8605-b0be68fe0d39

Security: https://gallagher.csod.com/ui/lms-learning-details/app/course/83cd67ec-4eb3-441c-b546-7e9f8d914c64

Incident and Violation Response Contacts:

Jennifer Ryder, Privacy Officer, will be the Gallagher contact person for receiving reports of privacy incidents and violations using the HIPAA Incident Form on BOSS:

These reports should be directed to:

Jennifer Ryder – General Counsel – Gallagher Benefit Servcies
2850 Golf Road

Rolling Meadows, IL 60008
Phone: 630-285-3833
e-mail: jennifer ryder@ajg.com

Link to HIPAA Incident Form on BOSS:
http://go.ajgco.com/gbs/BOSS/HWS/Pages/Privacy%20and%20Security%20Violation%20Procedure.aspx

James Downing, Security Officer, will be the Gallagher contact person for receiving reports of security incidents and violations as defined in the GITPSM-Security Incident Management (see link below).

Link to GITPSM-Security Incident Management:

https://go.ajgco.com/apps/itpolicy/Pages/viewpolicy.aspx#2.11.

These reports should be directed using the Incident Report Form on Gallagher One (see link below):

James Downing – Divisional Chief Technology Officer
2850 Golf Road
Rolling Meadows, IL 60008-4050
Phone: 630 285 4430
e-mail: james_downing@ajg.com

Security Related Incidents and Violations-Link to Incident Report Form on Gallagher One:

https://corpteams.ajgco.com/it/gts/apps/IncidentReporting/Lists/Security%20Incident%20Report%20Form/Draft.aspx

Sanctions for Violations of Policy

Sanctions for using or disclosing PHI/PII in violation of this Privacy and Security Policy will be imposed, up to and including termination of employment. Inadvertent use or disclosure of PHI/PII will be subject to a verbal or written warning. Blatant and purposeful use or disclosure without regard for this Policy will cause an individual to be subject to termination of employment.

Mitigation of Inadvertent Disclosures of PHI/PII

Gallagher shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of an individual's PHI/PII in violation of this Policy. As a result, if an employee becomes aware of an improper use or disclosure of PHI/PII, either by another Gallagher employee or an outside service provider/contractor that is not in compliance with this Policy, the employee is required to immediately contact the Privacy Officer so that the appropriate

steps to mitigate the harm to the participant can be taken. Please contact the Privacy Officer using BOSS link as follows:

https://go.ajgco.com/gbs/BOSS/HWS/Pages/Privacy%20and%20Security%20Violation%20Procedure.aspx

Privacy Guidelines

Gallagher shall exercise reasonable care to:

- Limit use or further disclosure of PHI/PII other than as permitted by business associate or confidentiality agreements in place with clients' health plans or insurance carriers or as required by law;

- Ensure that any agents or subcontractors to whom it provides PHI/PII received from covered entities, clients or insurance carriers agree in writing to the same restrictions and conditions that apply to Gallagher;

- Not use or disclose PHI/PII in connection with any other employee benefit plan;

- Report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures using the **HIPAA Incident Form on BOSS-Link:** http://go.ajgco.com/gbs/BOSS/HWS/Pages/Privacy%20and%20Security%20Violation%20Procedure.aspx

- Make Gallagher internal practices and records relating to the use and disclosure of PHI received from covered entities available to DHHS upon request (HIPAA specific requirement); and

- If feasible, return or destroy all PHI/PII received from covered entities/clients that Gallagher 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 feasible.

This Policy informs the Gallagher workforce that Gallagher has access to PHI/PII in connection with its daily business operations. The Policy also provides a description of the Gallagher violation procedures and the names and telephone numbers of individuals to contact for further information.

Security Guidelines

The purpose of this section is to communicate certain procedures used by Gallagher to protect the security of PHI/PII in accordance with the GITPSM (see link below). Gallagher intends to take all reasonably necessary steps to ensure that the PHI/PII it collects, maintains, uses or transmits is properly protected. For purposes of these security guidelines, "electronic media" shall mean electronic storage media including memory in computers (e.g. hard drives) and any

removable/transportable digital memory medium such as magnetic tapes or disks, optical disks, memory cards or transmission media used to exchange information (internet, leased lines, dial-up, intranets, private networks).

Link to GITPSM: https://go.ajgco.com/apps/itpolicy/SitePages/Home.aspx
Gallagher senior management shall regularly perform systematic assessments of potential risks and vulnerabilities pertaining to the confidentiality, integrity and availability of PHI/PII. These assessments shall include an evaluation of the communications with industry business partners and clients. Current policies and procedures to prevent, detect, contain and correct violations of the security standards and PHI/PII are also reviewed and updated as deemed appropriate by the Gallagher Security Officer.

Policies and procedures are used to ensure that access is granted only to authorized Gallagher personnel. Attached to provide further information and documentation regarding security guidelines is the Gallagher Security Guidelines section of this Policy.

Each Gallagher Branch location has a business continuity plan/disaster recovery plan which will be implemented in an emergency situation. This includes power outages, fires, hurricanes or tornados that could render the records inaccessible for a period of time or damage the files. Gallagher has policies and procedures in place to address the recovery and/or retrieval of the information during the emergency situation and Gallagher will control PHI/PII during an emergency situation. Gallagher requires that all Branches are secured against unauthorized access and in most cases the Branches will remain secured in an emergency. In the event of an emergency that exposes the building to unauthorized access, a security firm will be employed to protect the contents of the building until such time that the contents are removed to a secure location. The Gallagher Privacy Officer may be contacted to obtain specific information relating to the business continuity plan/disaster recovery plan.

Gallagher's contracts and other arrangements with business partners and clients allow Gallagher to receive, maintain or transmit PHI/PII and requires acknowledgment of the other party's duty to comply with all applicable rules and regulations regarding confidential and private information, including PHI and HIPAA security standards. Gallagher shall implement physical safeguards that deal with the electronic systems, equipment and workstations of its facilities. (see link below).

Link to GITPSM-Physical Security: https://go.ajgco.com/apps/itpolicy/Pages/viewpolicy.aspx#3.5

These safeguards limit physical access to the PHI/PII to ensure that it is controlled and monitored. This is accomplished by using physical barriers to protect workstation equipment (including the use of keycards) and validating access to information by the installation of password protection processes. All supervisors are trained to monitor access to PHI/PII and to take proper action if impermissible access occurs.

As noted herein and in the GITPSM (see link below), Gallagher shall monitor the destruction of PHI/PII to ensure that it is not destroyed in an unauthorized manner. Any recognized vulnerabilities or weaknesses in processes or procedures relating to the security and destruction of

PHI/PII shall be immediately addressed in a manner deemed appropriate by the Gallagher Security Officer.

Link to GITPSM: https://go.ajgco.com/apps/itpolicy/SitePages/Home.aspx

Documentation

Gallagher's Privacy and Security Policy and related procedures will be documented and maintained in accordance with the Gallagher Records Retention Policy. (see link below) Policies and procedures will 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 will be properly documented.

If a change in law impacts the Privacy and Security Policy, it will promptly be revised and made available. Such change is effective only with respect to PHI/PII created or received after the effective date of the notice unless specifically stated otherwise in the statutory language.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

Link to Gallagher Records Retention Policy:
https://go.ajgco.com/gbs/BOSS/HWS/Pages/Records-Retention-Policy.aspx

Policies on Use and Disclosure of PHI/PII

Use and Disclosure Defined

Gallagher will use and disclose PHI/PII only as permitted under applicable law. The following table contains definitions of the terms "Use" and "Disclosure" as applicable to PHI and PII, respectively.

	PHI (HIPAA)	PII
"Use"	The sharing, employment, application, utilization, examination or analysis of PHI by any person working for or within Gallagher, by another business associate of a covered entity or by a third party service provider to whom Gallagher has delegated a portion of its daily business operations. Use of PHI information should only be provided to or accessed by those who need it to perform their assigned job responsibilities.	The sharing of PII by any person working for or within Gallagher or by a third party to whom Gallagher has delegated a portion of its operations, who has a legitimate business need to know the information to accomplish a job function.
"Disclosure"	Any release, transfer, provision of access to or divulging of PHI in any manner to persons within Gallagher who would not	Any transfer or sharing of PII to persons within Gallagher who would not otherwise

	otherwise have access and to persons not employed by or working within Gallagher.	have access and to persons not employed by or working within Gallagher.

Compliance with Gallagher Policy and Procedures

All members of the Gallagher workforce (described at the beginning of this Policy and referred to herein as "employees") must comply with this Policy and with the Gallagher use and disclosure of PHI and PII procedures which are set forth in this document.

	PHI (HIPAA)	**PII**
Permitted Uses and Disclosures	Generally - Employees may use and disclose PHI to other covered entities and business associates of covered entities, and they may disclose PHI to other Gallagher employees (but the PHI disclosed must be limited to the minimum amount necessary to perform the necessary functions) Mandatory Disclosures - An individual'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; ▪ The disclosure is made to the Secretary of the Dept. of Health and Human Services ("Secretary") for purposes of enforcing HIPAA; Disclosure to an individual will apply only in those cases where Gallagher is the sole repository of original PHI. If an employee receives a subpoena or similar request from a public agency, it should be referred to the branch manager immediately for further handling. Permissive Disclosures - PHI may be disclosed for legal and public policy purposes without an individual's authorization, when specific requirements are satisfied. Requests of this nature should be referred to the Privacy Officer for handling:	Generally - PII may be used and disclosed by Gallagher employees to other Gallagher employees or to third parties only to the extent required to fulfill the services, functions and responsibilities for which such PII was provided to Gallagher or as required by law. Mandatory Disclosures – PII must be disclosed to a regulatory body as required by applicable law. PII must also be disclosed to the individual to whom such PII relates, but only if Gallagher is the sole repository of such PII and the individual's identity has been confirmed. If an employee receives a subpoena or similar request from a public agency, it should be referred to the Branch Manager immediately for further handling. Permissive Disclosures - PII may be disclosed for legal and public policy purposes without an individual's authorization, when specific requirements are satisfied. Requests of this nature should be referred to the Privacy Officer for handling.

	• Pursuant to legal process and as otherwise required by law; or • As necessary to alert law enforcement to the commission and circumstances of a crime. 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 individual who is the subject of the disclosure. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization. Disclosures of PHI for Payment and Health Care Operations – HIPAA states that PHI may only be disclosed for payment and health plan operation purposes and only where a Business Associate Agreement is in effect and subject to this Privacy and Security Policy. Payment – Payment includes activities undertaken to obtain health plan contributions or to determine or fulfill a health plan's responsibility for provision of benefits under the plan to plan participants, 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 – PHI may be disclosed for purposes of a health plan's operations. PHI of one covered entity 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 first health plan and the PHI requested pertains to that relationship. Health care operations mean any of the following activities to the extent that they are related to a particular entity: • 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; • Strategic business planning and development; and • Business management and general administrative activities <u>PHI may NOT be used or disclosed</u> for the payment or operations of "non-health" benefits (e.g., disability, life insurance, etc.) unless the health plan 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. In certain circumstances, PHI may be disclosed for purposes of administering a client's workers' compensation plan. In these cases, Gallagher should direct the client to request the disclosure of the PHI directly from the organization holding original data.	

Generally, employees working on a client team do not have access to other client's PHI/PII except when serving in a backup capacity to maintain normal Gallagher operations. Under certain circumstances (e.g. judicial or administrative proceedings), PHI/PII may be shared with employees in AJG Corporate Legal and/or Internal Audit who are bound by the terms of their corporate confidentiality agreement and professional code of ethical conduct.

Complying with the "Minimum-Necessary" Standard – PHI and PII

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.

Under HIPAA, 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 governing regulatory authority;
- Uses or disclosures required by law; or
- Uses or disclosures of PHI required to comply with HIPAA Electronic Data Interchange

For purposes of this Policy, when PII is used or disclosed it must also be limited to the "minimum necessary."

Minimum Necessary when Gallagher is Disclosing PHI/PII

For making routine and recurring disclosures of PHI/PII the following applies:

Routine and Recurring Disclosure	Recipient(s)	Gallagher Policy and Procedure
Health Plan Marketing	All Carriers, Health Plans	Provide summary and de-identified information initially; Provide PHI/PII only at final negotiation if required; Provide minimum necessary PHI/PII for accurate underwriting.
Budgeting and Renewal	Health Plan	Provide summary and de-identified information initially; Provide PHI/PII only at final negotiation if required; Provide minimum necessary PHI/PII for accurate underwriting.
Claim Issue Resolution	Health Plan, Plan Sponsor, Carrier/Provider, Third Party Administrator (TPA)	First, direct individual to plan representative or carrier/Third Party Administrator (TPA); Second, obtain authorization from individual.
Billing Issue Resolution	Health Plan, Plan Sponsor, Carrier/Provider, TPA	First, provide minimum necessary billing and enrollment data to resolve the issue; Second, obtain authorization from individual.
Compliance Issue Resolution	Outside Legal	Provide minimum details of PHI/PII necessary to secure legal opinion.
Strategic Planning	Plan Sponsor	Disclosure is not permitted.

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

Minimum Necessary When Gallagher is Requesting PHI/PII

For making routine and recurring requests for disclosure of PHI/PII the following applies:

Routine and Recurring Requests	Disclosing Entity	Gallagher Policy and Procedures

Health Plan Marketing	Health Plan, TPA, Insurance Carrier	Request summary and de-identified information and PHI/PII only if required
Renewal Underwriting and Experience Evaluation	Health Plan, TPA, Insurance Carrier	Request summary and de-identified information and PHI/PII only if required
Claims Audit	TPA, Insurance Carrier	Request summary and de-identified information and PHI/PII only if required
Claim Issue Resolution	Health Plan, TPA, Insurance Carrier	Request summary and de-identified information and PHI/PII only if required
Billing Issue Resolution	Health Plan, TPA, Insurance Carrier	Request summary and de-identified information and PHI/PII only if required
Compliance Issue Resolution	Health Plan, TPA, Insurance Carrier, Individual Outside Legal	Request summary and de-identified information and PHI/PII only if required
COBRA Rate or Funding Level Determination	Health Plan, TPA, Insurance Carrier	Request summary and de-identified information and PHI/PII only if required
Network Discount Evaluation	Health Plan, TPA, Insurance Carrier	Request summary and de-identified information and PHI/PII only if required
Disruption Analysis	Health Plan, TPA, Insurance Carrier	Request summary and de-identified information and PHI/PII only if required
Strategic Planning	Health Plan, TPA, Insurance Carrier	Request summary and de-identified information and PHI/PII only if required

All other requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Disclosures of PHI/PII to Service Providers and Third Parties (Subcontractors)

PHI (HIPAA)	PII
Under HIPAA, employees may disclose PHI to service providers and other third parties to which Gallagher has delegated a portion of its daily business operations. However, prior to doing so, employees must first obtain written documentation from the service provider or third party that it will appropriately safeguard the PHI according to the same standards that Gallagher does.	Employees may disclose PII to service providers and other third parties to which Gallagher has delegated a portion of its daily business operations to the extent required to fulfill the services, functions and responsibilities for which such PII was provided to Gallagher. However, prior to doing so, employees must first obtain written agreement from the service provider or third party that it will appropriately safeguard the PII according to the same standards that Gallagher does.

Before sharing PHI/PII with outside service providers and third parties (i.e. technical consultants, contractors, auditors, etc.), an employee must contact the Privacy Officer to verify that the service provider or third party has a recognized business relationship with Gallagher and an appropriate confidentiality/nondisclosure agreement is in place.

Disclosures of PHI/PII to Other Business Associates or Authorized Plan Vendors

PHI (HIPAA)	PII

Employees may disclose PHI to other business associates, such as TPAs and other pharmacy benefit managers, of a particular covered entity in order to conduct the daily business operations of Gallagher. However, prior to doing so, employees must first verify with the covered entity that a business associate contract is in place between the covered entity and the organization purporting to be a business associate of the covered entity. Under HIPAA, a Business Associate is an entity that: ▪ Performs or assists in performing a function or activity for or on behalf of a covered entity involving the use and disclosure of PHI (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 services provider access to PHI.	Employees may disclose PII to authorized vendors of the respective client in order to fulfill the services, functions and responsibilities for which such PII was provided to Gallagher. However, prior to doing so, employees must first confirm with the client that the vendor is in fact authorized to receive such PII.

Disclosures of De-Identified Information and Limited Data Sets

PHI (HIPAA)	PII
De-Identification - Under HIPAA, whenever possible, Gallagher shall de-identify PHI in accordance with 45 C.F.R. § 164.514. Such 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. To de-identify information, 18 specific identifiers ***must*** be removed. 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 number • Health plan beneficiary numbers • Account numbers • Certificate/license numbers • Vehicle ID and serial numbers, including license plate numbers • Device identifiers and serial numbers • Web Universal Resource Locators (URLs)	Whenever possible, Gallagher shall de-identify materials containing PII prior to making disclosures to third parties by removing the PII from the materials, or otherwise striking through such PII so that it is not recognizable to the recipient and the identity of the individual to whom the PII applies cannot be reasonably inferred by the recipient by either direct or indirect means. There are no specific identifiers that must be removed for PII to be considered adequately de-identified.

• 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 Limited Data Sets- Under HIPAA a Limited Data Set is PHI that excludes 16 direct identifiers of an individual. Gallagher may disclose Limited Data Sets for purposes of research, public health or health care operations only after it has obtained satisfactory assurances, in the form of a data use agreement, from the recipient (in accordance with 45 C.F.R. § 164.514(e)). The 16 identifiers that ***must*** be excluded are: • Names • Postal address information, other than town or city, state and zip code • Telephone numbers • Fax numbers • Electronic mail addresses • Social Security numbers • Medical record number • Health plan beneficiary numbers • Account numbers • Certificate/license numbers • Vehicle ID 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	

If there is any question as to whether data has been appropriately de-identified in compliance with these guidelines, contact the Privacy Officer for assistance.

PHI/PII Protection

PHI/PII Storage and Access

The HIPAA Privacy Rules and applicable state laws require that Gallagher implement and maintain appropriate administrative, technical and physical safeguards to protect the privacy of ePHI and PHI. More specifically, Gallagher must have in place reasonable safeguards to protect ePHI and PHI, from intentional or unintentional use or disclosure that is in violation of applicable law. Accordingly, Gallagher adopts and complies with the electronic storage, access and media disposal provisions of the GITPSM.

In addition, physical protection of PHI/PII will be maintained through various means as follows:

- Primary Physical Protection – provide a secure reception area and do not leave visitors unattended.
- Secondary Physical Protection – provide a separate file area or enclosed room for file storage. Separate Gallagher files from those of other divisions that are co-located in the office.
- Verbal – Employees shall take reasonable care in verbally discussing a covered entity or client's PHI/PII to ensure that PHI/PII is not discussed with any employee, individual or third party who should not have access to PHI/PII per the terms of this Policy. (Also, employees should be mindful of engaging in conversations or telephone calls in areas that do not provide reasonable privacy for the conversation.)
- Maintenance – Branch Privacy Coordinators (BPCs) will monitor physical and verbal protection of PHI/PII and access to Gallagher files. Each BPC will report any privacy incident or violation to the Gallagher Privacy Officer as soon as possible. In those offices where Gallagher shares space with other Gallagher divisions such as BSD, or outside corporations, the BPC will take reasonable measures to ensure that no employees from those other entities obtains access to Gallagher files.
- Destruction of PHI/PII – When it becomes necessary to discard PHI/PII, employees should take reasonable care to ensure that PHI/PII is left completely inaccessible. PHI/PII in any physical form (e.g. hard copy) may not be discarded in ordinary trash or recycle bins. Paper documents containing PHI/PII should be shredded whenever possible, or placed in a locked bin designated as a secure disposal receptacle.

Gallagher branch offices shall engage a service to pick up and destroy PHI/PII on a regular basis. If this is not feasible, then a cross-cutting shredder shall be used by the branch to destroy PHI/PII on a regular basis by a specific person who has access to PHI/PII and is designated to perform this function. In either case, discarded PHI/PII should be kept in an easily accessed, locked receptacle in the office until the PHI/PII is destroyed by the branch or picked up by the service provider.

PHI/PII Storage – Lost or Terminated Clients

PHI (HIPAA)	PII
PHI of lost and/or terminated covered entity clients shall be protected in the same manner as it was prior to termination. Under HIPAA, if Gallagher determines that returning or destroying the PHI is infeasible (including	PII of lost and/or terminated clients shall be protected in the same manner as it was prior to termination. If return or destruction of the PII is not feasible for any reason, the client should be made

the imposition upon Gallagher of an undue financial burden), then Gallagher will notify the client within a reasonable period of time after the termination becomes known to Gallagher (or within any specific time period indicated in the applicable BAA) of the conditions that make return or destruction infeasible. The HIPAA BAA Termination Letter template located in BOSS can be used for purposes of notifying a lost/termed covered entity client that return or destruction of PHI is infeasible. Unless otherwise specified in the covered entity client's BAA, upon mutual agreement with the covered entity client, Gallagher will limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for as long as Gallagher maintains such PHI. **(see link below to HIPAA BAA Termination Letter template):** https://go.ajgco.com/gbs/BOSS/HWS/Pages/Business-Associate-Termination.aspx	aware as a courtesy within a reasonable period of time after the termination becomes known to Gallagher.

In all cases, Gallagher must maintain those client records including PHI/PII that are necessary to meet business operational standards, including corporate policy and legal requirements for record retention and storage.

PHI/PII Transmission

Mail

Incoming postal mail should be delivered unopened in its original sealed envelope to the person to whom it is addressed. Employees should request that their business contacts clearly indicate the name of a specific person at Gallagher on the envelope. IF an employee receives PHI/PII inadvertently, the employee should redirect the incoming mail as soon as possible to an appropriate person who was intended to have access to such PHI/PII.

Outgoing postal mail shall be clearly addressed to a specific person at the organization where it is sent who is permitted to access PHI/PII per the organization's instruction, and marked "Personal and Confidential".

Email (including faxes sent via email) can be used by Gallagher employees to send ePHI/PII, however the ePHI/PII must be sent in an encrypted format using the current e-mail encryption process. Additional information regarding the use and transmittal of ePHI can be found in the GITPSM and specific information regarding the current e-mail encryption process can be found on the HIPAA Secure E-Mail Process section of the Gallagher Business Operating Standards and Systems (BOSS) portal. (see link below).

Link to Gallagher current e-mail encryption process:
https://go.ajgco.com/gbs/BOSS/HWS/Pages/Secure%20Email%20Process.aspx

Printer

Printers must be kept in an enclosed area or room to limit access to incoming communications (i.e. not the reception area). Employees should exercise reasonable care to keep printed documents secure and limit access by other Gallagher employees, divisional employees or outside organizations that share office space with Gallagher. If an employee finds a document containing PHI/PII left on the printer inadvertently and the employee should not be accessing the particular PHI/PII, the employee should redirect the document as soon as possible to the appropriate person or destroy it in a manner permitted under this Policy.
Additional information relating to the storage, access and transmittal of PHI/PII is available in the **Gallagher Benefit Services (GBS) Privacy and Security Procedures (HIPAA – PHI and PII) found on BOSS (see link below)**.

Link to GBS Privacy and Security Procedures (HIPAA-PHI and PII):

http://go.ajgco.com/gbs/BOSS/HWS/Pages/Privacy%20and%20Security%20Violation%20Procedure.aspx

Incidents or Violations Policy

Notification of Potential Violation of Privacy and Security Policy

Any employee who suspects or believes a potential violation of this Privacy and Security Policy has occurred is required to immediately contact either the Security or Privacy Officer, their designees (depending on the type of violation) or the Branch Privacy Coordinator and should report the incident or violation as follows:

1) **Security Related Incidents and Violations-Link to Incident Report Form on Gallagher One:** access the Gallagher One Portal and complete an online form titled "Incident Report Form", (see link below) in accordance with the AJG Incident Response and Contact Procedure (see link below) for the reporting of security related incidents or violations;

   Link to Incident Report Form on Gallagher One:

   https://go.ajgco.com/apps/itpolicy/Pages/viewpolicy.aspx#2.11

   Additional information regarding incident report and contacts: Link to AJG Incident Response and Contact Procedure:

   https://go.ajgco.com/apps/itpolicy/Pages/viewpolicy.aspx#2.11.

2) **HIPAA and Privacy Related Incidents and Violations-Link to HIPAA Incident Form on BOSS:** access the "HIPAA Incident Report Form" found on BOSS (see link below) for the reporting of HIPAA or privacy related incidents or violations;

Link to HIPAA Incident Form on BOSS:
http://go.ajgco.com/gbs/BOSS/HWS/Pages/Privacy%20and%20Security%20Violation%20Procedure.aspx

In a confidential manner, the Security or Privacy Officer will investigate the facts and circumstances of the alleged violation and determine an appropriate course of action.

If the potential violation involves PHI, HIPAA sets forth a very specific notification procedure for both Privacy and Security violations, as set forth in Section (1) below. If the potential violation involves PII, notifications are still required by applicable law as set forth in Section (2) below, but the content and timing of those notices is not as precisely specified as in the HIPAA rules.

(1) HIPAA Specific Procedures Applicable to Privacy and Security Incidents or Violations Involving PHI

Notification of HIPAA Security Incident (HIPAA Security Rule - PHI)

Under the HIPAA Security Rule, a Security Incident is defined as:

> *The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system (45 C.F.R. Part 164.304).*

Any Security incident (as defined above) shall be properly reported to the respective covered entity by the Gallagher Security or Privacy Officer as soon as reasonably practicable, but not later than 2 business days from the date Gallagher becomes aware of the incident, unless a report is required sooner pursuant to the terms of the governing agreement with the applicable covered entity. Said report to the covered entity will contain the following:

- A description of the risk assessment performed and Gallagher's conclusion whether the disclosure is or may be a breach.
- Explanation of the date of the occurrence, date discovered and how discovered.
- Explanation of the general nature of the PHI involved without additional disclosure.
- Recommended steps to protect and mitigation options that Gallagher will provide to the individuals whose PHI is affected.
- An explanation of how Gallagher is investigating and mitigating the risk of future disclosures and a description of any sanctions of Gallagher's workforce members.
- Gallagher will provide the covered entity any information it may need to maintain a record of compliance with notification requirements including a sample of the notification(s) that the business associate was required to make pertaining to the covered entity. The

information will include a list of the affected members of the covered entity receiving the notification and a sample of the agreed notification content for the covered entity's records.

Notification of Breach (HIPAA Privacy Rule – PHI)

Under the HIPAA Privacy Rule, a Breach is defined as:

The unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information. However, the term Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

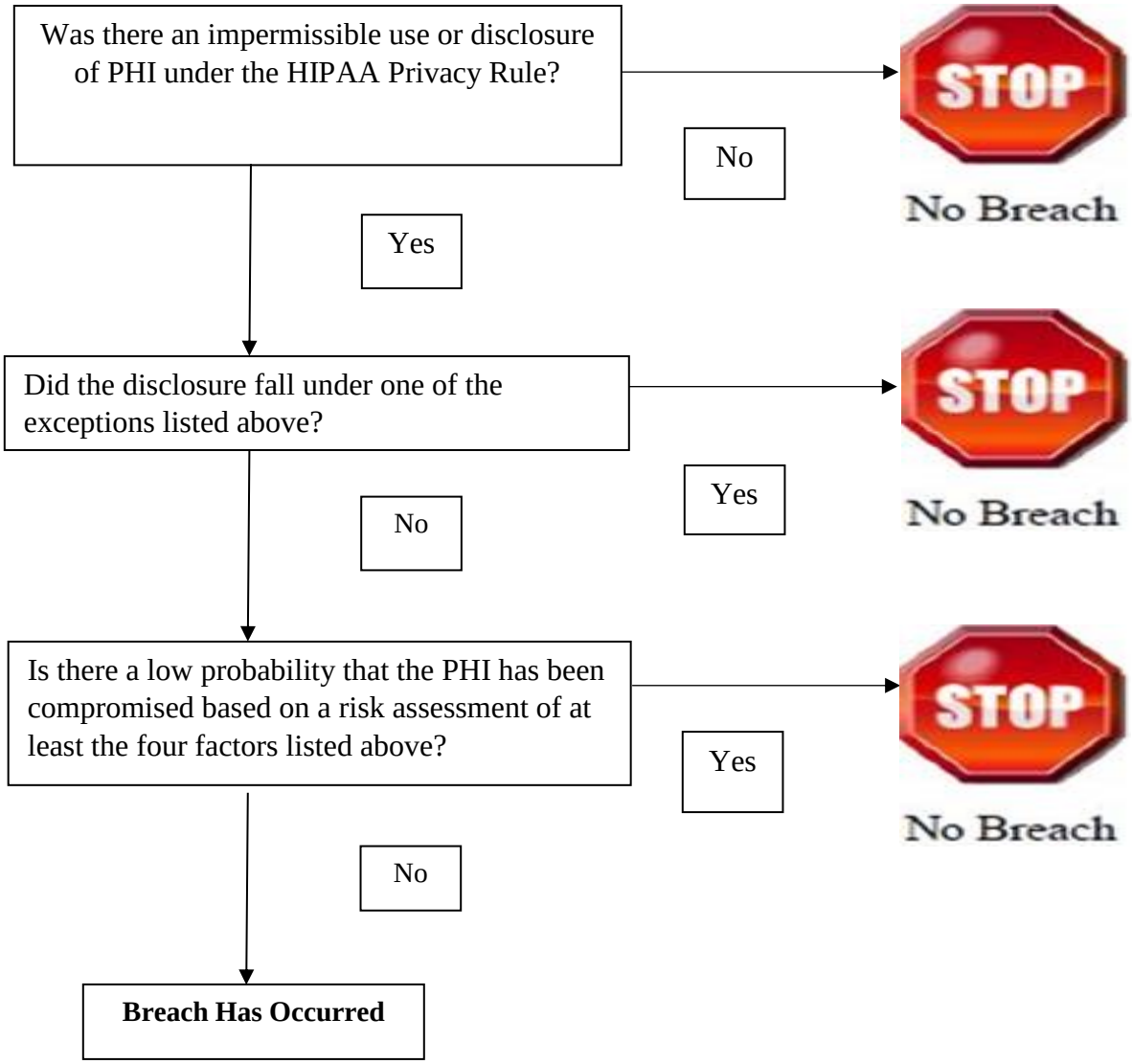
(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Except with regard to the three exclusions listed above, any unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information is presumed to be a Breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. *The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;*
2. *The unauthorized person who used the protected health information or to whom the disclosure was made;*
3. *Whether the protected health information was actually acquired or viewed; and*
4. *The extent to which the risk to the protected health information has been mitigated.*

(45 C.F.R. Part 164.402)

The flow chart and questions below should be considered by the Privacy Officer before determining whether an event constitutes a HIPAA Breach:



ANALYSIS TO DETERMINE IF AN EXCLUSION TO THE HIPAA DEFINITION OF BREACH APPLIES	
Nature of the recipient	Was PHI exposed to another Covered Entity or Business Associate?
	Was the recipient acting in good faith?
	Was the recipient a person who is otherwise authorized to access PHI?
Nature of the sender and recipient	Is sender an authorized person in a Covered Entity or Business Associate?
	Is recipient an authorized person in a Covered Entity or Business Associate?
	Did both parties otherwise adhere to the Privacy Rule?
	Was the recipient unable to retain the PHI?

Even if the Privacy Officer determines that a Breach has occurred, notification of such Breach may not be required. DHHS (45 CFR §§ 164.402) provides the following guidance:

> *Covered entities and business associates must only provide the required notifications if the Breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.*

When Gallagher is responsible for a Breach that requires notification, Gallagher will perform all required notifications in accordance with the HIPAA Breach Notification Rule; first notifying the covered entity and then, upon mutual agreement that a Breach requires notification, will issue the required notifications. Note, if the Breach involves more than 500 individuals, then notices to the affected individuals, the media, and/or DHHS may be required. Furthermore, Gallagher will provide evidence to the covered entity of having fulfilled the notification requirements pertaining to the covered entity.

The notification to the covered entity shall contain, as appropriate, the following information (45 CFR §§ 164.402):

- The nature of the non-permitted access, use or disclosure, including the date of the Breach and the date of the discovery of the Breach;
- The PHI accessed, used or disclosed as part of the Breach;
- Who or what office or department of operation made the non-permitted access, use or disclosure and who received the non-permitted disclosure;
- What corrective action Gallagher took or will take to prevent further non-permitted accessed, uses or disclosures;
- What Gallagher did or will do to mitigate any injurious effect of the non-permitted access, use or disclosures;
- Other information as may be reasonably requested by covered entity or required by HITECH regulations or regulatory entities; and
- Provide covered entity immediate notification and information related to any written inquiry received by Gallagher regarding a Breach from a regulatory entity.

(2) Procedures Applicable to Privacy and Security Incidents or Violations Involving PII

Notification of Security or Privacy Incident or Violation (PII)

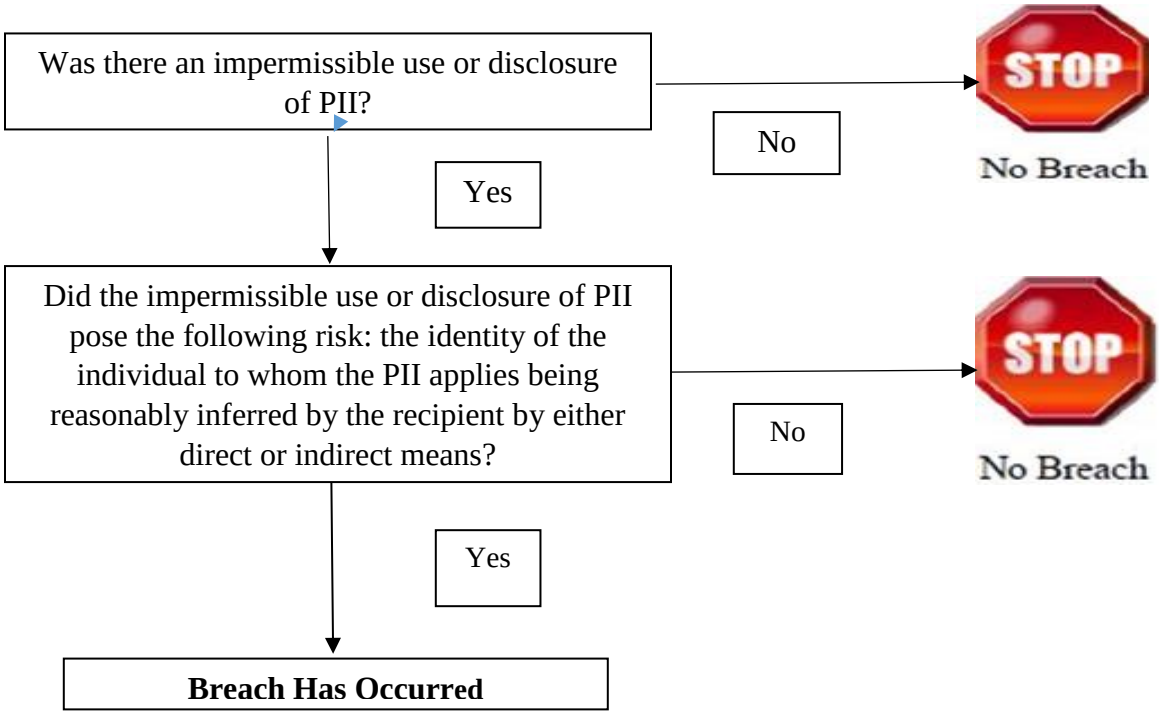
Any security or privacy incident or violation involving the unauthorized disclosure of PII shall be properly reported to the respective client by the Gallagher Security Officer or Gallagher Privacy Officer as soon as reasonably practicable, but not later than 10 business days from the date Gallagher becomes aware of the incident or violation, unless a report is required sooner pursuant to the terms of any existing agreement between Gallagher and the client in question. Said report to the client will contain substantially the following information:

- A description of the risk assessment performed and Gallagher's conclusion whether the disclosure is or may be a breach.
- Explanation of the date of the occurrence, date discovered and how discovered.
- Explanation of the general nature of the PII involved without additional disclosure.
- Recommended steps to protect and mitigation options that Gallagher will provide to the individuals whose PII is affected.
- An explanation of how Gallagher is investigating and mitigating the risk of future disclosures and a description of any sanctions of Gallagher's workforce members.
- Gallagher will provide the client any information it may need to maintain a record that notifications were made, including a sample of the notification(s) that Gallagher was required to make pertaining to the client. The information will include a list of the affected members of the client receiving the notification and a sample of the agreed notification content for the client's records.

Notification of Security or Privacy breach (PII)

Each state has its own laws and regulations that define what constitutes a breach of PII. In general, for purposes of this Policy, a breach of PII is the unauthorized acquisition, access, use or disclosure of PII which compromises the security, privacy or integrity of such personal information. It does not include the good faith acquisition of PII by an employee or agent of Gallagher for a legitimate business purpose, provided that the PII is not used for any unrelated purpose and is not subject to further unauthorized disclosure.

The flow chart below should be considered by the Security or Privacy Officer before determining whether an event constitutes a breach of PII:



When Gallagher is responsible for a breach of PII that requires notification, Gallagher will perform all required notifications in accordance with applicable governing law; first notifying the client and then, upon mutual agreement that a breach requires notification, will issue the required notifications. Furthermore, Gallagher will provide evidence to the client of having fulfilled the notification requirements pertaining to it.

The notification to the affected client shall contain, as appropriate, the following information:

- The nature of the non-permitted access, use or disclosure, including the date of the breach and the date of the discovery of the breach;
- The PII accessed, used or disclosed as part of the breach;
- Who or what office or department of operation made the non-permitted access, use or disclosure and who received the non-permitted disclosure;
- What corrective action Gallagher took or will take to prevent further non-permitted accessed, uses or disclosures;
- What Gallagher did or will do to mitigate any injurious effect of the non-permitted access, use or disclosures;
- Other information as may be reasonably requested by the client or required by applicable governing law;
- Provide client immediate notification and information related to any written inquiry received by Gallagher regarding a breach from a regulatory authority.

Incident and Violation Resolution (applicable to violations involving both PHI and PII)

If it is determined that an incident or violation of the Gallagher Privacy and Security Policy has occurred, all relevant parties such as the employee(s), client, plan administrator, covered entity, and third party service provider will be notified in a timely manner. The resolution of any such incident or violation will seek to restore the level of security and/or privacy that is required under this Policy. Any deficiency in the Privacy and Security Policy or related procedures that contributed to the incident or 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 standard Gallagher disciplinary practices. Depending on the severity of the incident or violation and whether or not it 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 service provider, appropriate action will be taken to correct the situation and reevaluate the service provider

relationship with Gallagher up to and including termination of the relationship as provided for in the confidentiality agreement or other document governing the relationship.

Incident or Violation Tracking (applicable to violations involving both PHI and PII)

The Privacy and Security Officers 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. Furthermore, Gallagher will maintain a log of Breaches involving less than 500 individuals and after the end of each calendar year, if required by HITECH, notify the Secretary of Health and Human Services pursuant to its Breach Notification Requirements.

Exhibit A-General Security Guidelines

The following sections provide general detail on how Gallagher complies with the specific HIPAA Security Implementation Specifications. Additional questions regarding specific Gallagher security policies should be directed to James Downing, the Gallagher Security Officer.

Security Management Process
Gallagher adheres to various polices to prevent, detect, contain, and correct security violations.

	How Gallagher Complies
Risk Analysis	The Gallagher Security Officer, completed a thorough assessment of the potential risks and vulnerability to the confidentiality, integrity, and availability of ePHI held by Gallagher in accordance with the HIPAA Security regulations.

Risk Management	Gallagher implements security measures to reduce risks and vulnerabilities as identified in the Gallagher risk analysis and assessment to a reasonable and appropriate level.
Sanction Policy	Security violations will be addressed by a review of each case. Monetary damages, if due, will be settled under the laws of the state of Illinois. Employee(s) found responsible for the violation will be subject to disciplinary action that may range from verbal warning, written warning, and probations, up to and including termination of employment, legal action or both. The Security Officer, Gallagher 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 Security Officer and Gallagher Management will take appropriate action up to and including terminating service provider's relationship with Gallagher, legal action or both.
Information System Activity Review	Gallagher IT logs information system activity and retains collected information for review.

Workforce Security

Gallagher has policies and procedures to ensure that all staff have access to ePHI appropriate to the duties of their position and to prevent staff members who should not have access to ePHI from obtaining it.

	How Gallagher Complies
Authorization and/or Supervision	Department/branch management will determine the levels of supervision necessary based on the employee's access to ePHI and the sensitivity of that information.
Workforce Clearance Procedure	Branch Manager or designee will assign appropriate access to ePHI based on duties of the job function.
Termination Procedures	• Branch Manager or designee must request to modify, or delete user access to any information system. • Branch Manager or designee will also retrieve all keys, locks, etc. to office.

Information Access Management
Gallagher authorizes appropriate access to ePHI by limiting access to those employees that need it for business need.

	How Gallagher Complies
Access Authorization	Branch Manager or designee will evaluate the employee job title and duties to determine necessary access to ePHI.
Access Establishment and Modification	• Branch Manager or designee will request access via the AJG Identity Management System following the procedures as described in current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM). • Modifications of user access are performed by the Identity Management System or the appropriate technology owner or the data owner based on the direction of the Branch Manager or designee.

Security Awareness and Training
Gallagher has implemented the following required HIPAA Security Training for all employees.

	How Gallagher Complies
Security Awareness and Training	Using the AJG Cyber Security Awareness Training Module, Gallagher conducts annual security training for all employees. New hire training is required to be completed within 45 days of assignment. Training is mandatory and each employee is required to pass an evaluation demonstrating their understanding and responsibilities. Branch Managers and other managers are responsible for verifying all employees complete this training module within 45 days of assignment.
Security Reminders	Gallagher will send out periodic email alerts on any potential new risks (e.g. certain virus or worms, or changes to security policy)
Protection from Malicious Software	Training includes information on guarding against and detecting malicious software, viruses, worms, etc.
Log-in Monitoring	As part of Gallagher's IT security program, IT security logs login success/failure, and reports discrepancies.
Password Management	Gallagher has procedures for creating, changing and safeguarding passwords and are outlined in the current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM). Gallagher training will include these procedures as defined in current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM).

Business Associate Contracts and Other Arrangements

	How Gallagher Complies
Written Contract or Other Arrangement	• When Gallagher is a Business Associate to client Group Health Plans, Gallagher Branch Privacy Coordinators review Business Associate Agreements using Gallagher guidelines located in the Gallagher BOSS database and obtain the appropriate signature. • Gallagher does not have any Business Associates. • Gallagher requires subcontractors to sign an agreement to protect the security of a covered entity's ePHI

Contracts and Other Arrangements

Standard Evaluation

	How Gallagher Complies
Evaluation	Gallagher performs periodic technical and non-technical evaluations of the components of its security safeguards.

Contingency Plan
Gallagher has contingency plans to respond to emergency or other occurrences that damage systems that contain ePHI.

	How Gallagher Complies
Data Back-up	Gallagher maintains retrievable exact copies of ePHI. All Gallagher branches are required to follow corresponding processes: -Gallagher Business Continuity Plan/Disaster Recovery Plan. -the current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM)
Business Continuity Plan/Disaster Recovery Plan	Gallagher branches are required to complete and maintain a Business Continuity Plan/Disaster Recovery Plan. All Gallagher branches are required to follow corresponding processes: - Business Continuity Plan/Disaster Recovery Plan. -the current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM)
Emergency Mode Operation Plan	All Gallagher branches have an emergency mode operation plan that includes implementation of the Branch Business Continuity Plan/Disaster Recovery Plan and the current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM).
Testing and Revision Procedures	At least annually, Gallagher branches review and update the Gallagher Business Continuity Plan/Disaster Recovery Plan. The Gallagher branches also periodically test the contingency plan and make appropriate changes if necessary.
Applications and Data Criticality	Gallagher has determined which applications and data are necessary or are important for continuing its business operations.

Device and Media Controls

Gallagher adheres to the following policies to govern a facility's receipt and removal of hardware and electronic media that contain ePHI and the movement of these items into, out of, and within the facility.

	How Gallagher Complies
Disposal	Gallagher has policies and procedures regarding the disposal of hardware or software containing ePHI.
Media Re-use	Gallagher has policies and procedures about the re-use of media, such as USB storage, CDs/DVDs, and hardrives.
Accountability	Gallagher maintains inventory on all hardware, software and media within Gallagher.
Data Backup and Storage	Gallagher backs up all data before it is relocated or stored. Back-ups will occur according to the current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM)

Data Integrity
Gallagher adheres to the following policy to implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

	How Gallagher Complies
Mechanism to Authenticate ePHI	Backups will occur according to the current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM).

Person or Entity Authentication
Gallagher adheres to the following policy to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

	How Gallagher Complies
Person or Entity Authentication	Gallagher requires a unique user ID and password to all systems. IT assigns user ID and passwords according to the current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM)

ePHI Transmission Security
Gallagher adheres to the following policies to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

	How Gallagher Complies
Integrity Control	Gallagher employees transmit ePHI through Gallagher Insight, BenefitPoint, a Secured vendor site or Secure E-mail. All require a unique ID and password. Media devices such as CDs or USB Drives that include ePHI that are mailed and tracked by individual account teams.
Encryption	Gallagher transmits ePHI only through secured websites including Gallagher Insight, BenefitPoint, or a secured carrier site. Gallagher employees can send ePHI via e-mail however the ePHI must be contained in a password protected document or follow the Gallagher secure e-mail process.

Technical Access Controls
Gallagher adheres to the following policies to allow access only to persons or software that have been granted access rights.

	How Gallagher Complies
Unique User Identification	Gallagher IT is responsible for the user naming convention. It is required that users have a unique ID and complex password. Gallagher prohibits the use of shared IDs. Do not share IDs and passwords or use unauthorized passwords to gain access to unauthorized areas.
Emergency Access Procedure	Each Gallagher Branch is required to have a Business Continuity Plan/Disaster Recovery Plan that addresses an Emergency Access procedure.
Automatic Logoff	Gallagher requires the use of a locking screensaver after 15 minutes of inactivity that requires the use of a password to reenter once activated.
Encryption and Decryption	Gallagher laptops are encrypted. Gallagher also uses additional security measures which include physical security barriers including locks, keys and IT system security barriers including log-ons, restricted access, user IDs and passwords. Branches will ensure that physical access and electronic access is controlled in accordance with Gallagher security policies.

Technical Audit Controls
Gallagher adheres to the following policy to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems.

	How Gallagher Complies
Audit Controls	The following information is being logged and maintained in a central repository: • Account Misuse • High volume login attempts • All user logins on the servers • If a customized report is needed, the procedure is to contact Gallagher IT security and request the details of what the report should include. (Server name, directories/files, user name and date range)

Workstation Use
Gallagher adheres to the following policy to specify the proper functions to be performed, the manner in which those functions are to performed, and the physical attributes of the surroundings of a specific workstation or class of workstation.

	How Gallagher Complies
Workstation Use	• Access to workstation ePHI is limited to those employees who have been authorized by branch or department management. • Employees will lock their system or log off before leaving a workstation unattended or close screen displaying ePHI if unauthorized employees enter the work area.

Workstation Security
Gallagher adheres to the following policy to implement physical safeguards for all workstations and to restrict access to authorized users.

	How Gallagher Complies
Workstation Security	• Gallagher minimizes the possibility of unauthorized access to ePHI. • Offices are locked after business hours • Workstations are positioned to minimize the possibility of unauthorized viewing of screens. • Screens automatically lock after 15 minutes and require employees to unlock their system with their passwords. • Laptop computers have additional security measures to limit unauthorized access to ePHI and to prevent theft.

Facility Access Controls
Gallagher adheres to the following policies to limit physical access to systems and the facilities in which they are housed.

	How Gallagher Complies
Contingency Operations	The Gallagher Branch Business Continuity Plan/Disaster Recovery Plan addresses the procedures that allow facility access in support of restoration of lost data under the business continuity plan/disaster recovery plan. Branch Management are required to ensure its completeness and testing.
Facility Security Plan	Branch management safeguards the facility from unauthorized access and theft by following the current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM).
Access Control and Validation Procedures	Gallagher controls employee access to facilities and electronic systems. Visitors are required to be signed in and out and escorted by a Gallagher employee at all times.
Maintenance Records	Each Branch is responsible for having a designated person to respond and to track maintenance issues (i.e. building maintenance). Each time a repair or replacement is made to a security system (e.g. lock, card key systems, IT systems, etc.), it is each Branch's responsibility to maintain a log documenting what was done, who did it and when. Only designated approved personnel will be allowed to make necessary repairs. The Branch Manager or designee will approve all repairs prior to a maintenance request. All Gallagher branches are required to create and maintain a branch maintenance log and upload the log onto the Managers Library.

Information Access Management
Gallagher authorizes appropriate access to ePHI by limiting access to those employees that need it for business need.

	How Gallagher Complies
Access Authorization	Branch Manager will evaluate the employee job title and duties to determine necessary access to ePHI.
Access Establishment and Modification	• Branch Manager or designee requests access from the AJG Identity Management System following the procedures as described in the current version of the Arthur J. Gallagher Global IT Policies and Standards Manual Version (GITPSM). • Reviews and modifications of user access are initiated by the appropriate technology owner based on the direction of the Branch Manager or designee.

Security Management Process and Incident Procedures
Gallagher adheres to the following polices to prevent, detect, contain, and correct security sanctions.

	How Gallagher Complies
Sanction Policy	Security violations will be addressed by a review of each case. Monetary damages, if due, will be settled under the laws of the state of Illinois. Employee(s) found responsible for the violation will be subject to disciplinary action that may range from verbal warning, written warning, and probations, up to and including termination of employment, legal action or both. The Security Officer, Gallagher 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 Security Officer and Gallagher Management will take appropriate action up to and including terminating service provider's relationship with Gallagher, legal action or both.
Response and Reporting	Gallagher identifies and responds to suspected or known security incidents, and to mitigate, to the extent practicable, the harmful effects. All known incidents are documented along with the outcome by the Security Officer. **Reporting a Violation** Any employee who believes that a security violation as defined in this Policy has occurred is required to contact the Security Officer immediately to report the incident in question. The Incident form on Gallagher One should be used to document and report a suspected violation. The Security Officer or designee will investigate the facts and circumstances of the alleged violation and determine an appropriate course of action. **Violation Resolution** The Security Officer will notify all involved parties, such as, employee(s), client, plan administrator, covered entity, and third party provider, in a timely manner once it has been determined that a violation of this Policy has occurred. The resolution of any such violation will seek to restore the level of security that is required under this Policy. The Security Officer will correct any deficiency in this Policy or related procedures. **Violation Tracking** The Security Officer will maintain relevant information on Gallagher One on all reported incidents of potential violation under this Policy whether or not a reported incident is ultimately found to be an actual violation. The violation log will be used to track reported violations.