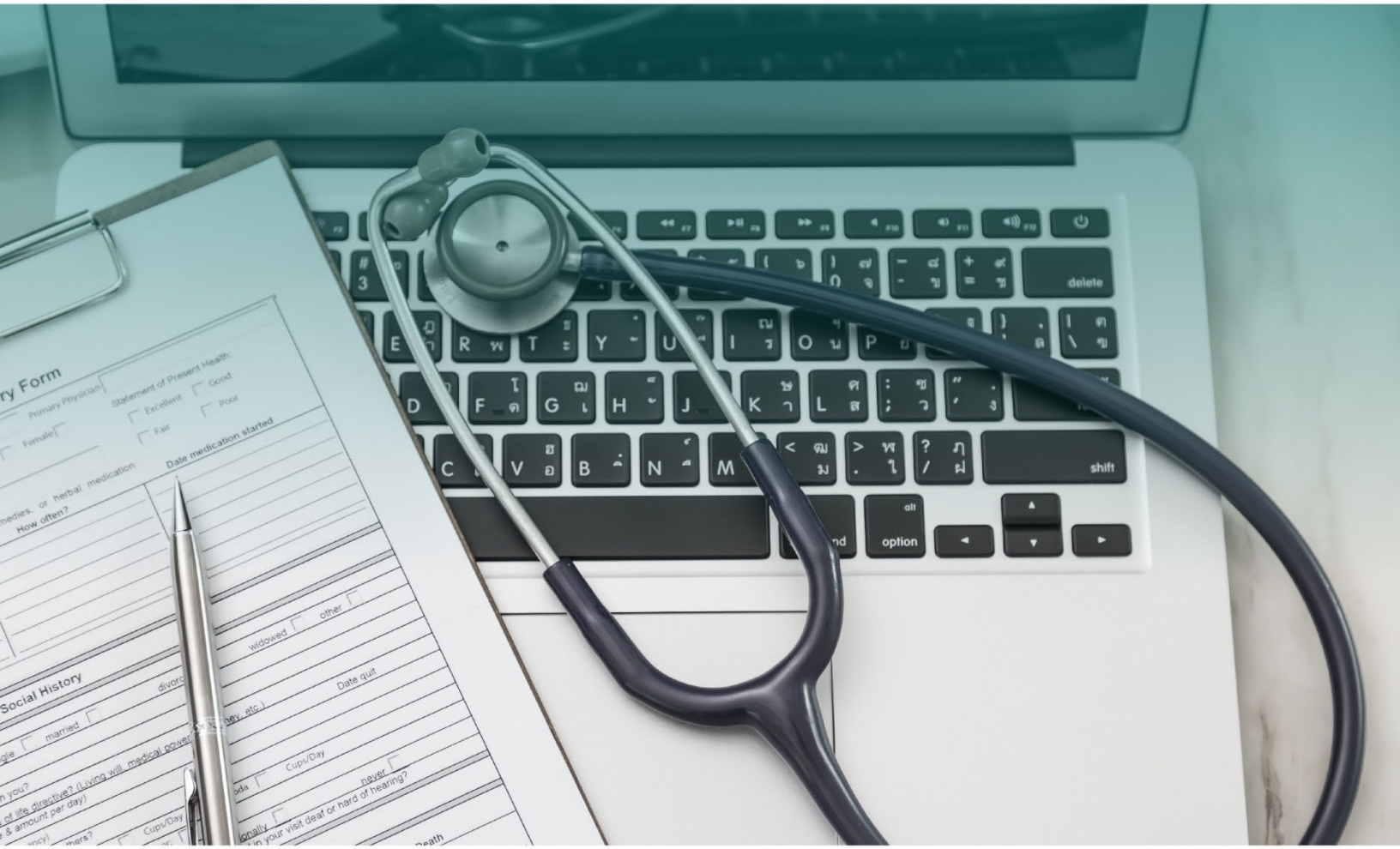
HIPAA PRIVACY AND SECURITY COMPLIANCE TOOLKIT

Provided by **Lawley**



Lawley

TABLE OF CONTENTS

INTRODUCTION

This toolkit is intended to help employers that sponsor group health plans understand their compliance obligations under the Health Insurance Portability and Accountability Act (HIPAA). It also provides sample resources to help employers comply with HIPAA's documentation requirements for their group health plans.

WHAT THIS TOOLKIT COVERS

HIPAA is a broad federal law that includes rules for protecting the privacy and security of certain health information, which is called protected health information (PHI). HIPAA also includes notification requirements following a breach of PHI. This toolkit discusses the following rules, which are collectively referred to as the **HIPAA Rules**:

HIPAA Privacy Rule	HIPAA Security Rule	HIPAA Breach Notification Rule
• Sets national standards for when PHI may be used or disclosed • Gives individuals certain rights with respect to their PHI	• Includes standards that covered entities must implement to protect their electronic PHI (ePHI)	• Requires covered entities to notify affected individuals, the Department of Health and Human Services (HHS) and, in some cases, the media, following a breach of unsecured PHI

While employers are not directly regulated by the HIPAA Rules, most employer-sponsored group health plans are subject to the HIPAA Rules' requirements to some degree. This means that employers that sponsor group health plans for their employees will usually have compliance obligations under the HIPAA Rules with respect to their group health plans. The extent of an employer's compliance obligations under the HIPAA Rules mainly **depends on two factors**:

- ✓ Whether the employer's health plan is **self-funded or fully insured**; and
- ✓ If the health plan is fully insured, whether the employer has **access to PHI** from the health insurance issuer (other than certain limited types of PHI).

KEY POINTS

- If an employer receives PHI from its health plan (for example, from the issuer or benefits administrator), the employer takes on ***significant responsibilities*** with respect to that PHI.
- Employers that sponsor **fully insured health plans** and **do not have access to PHI** (other than certain limited types) from their issuers have ***minimal compliance obligations*** under the HIPAA Rules.

ADDITIONAL RESOURCES

HHS RESOURCES

In addition to this toolkit, there are resources available from HHS to help covered entities comply with the HIPAA Rules. These resources are available through HHS' website on the following topic pages:

- Guidance on the HIPAA Privacy Rules
- HIPAA Security Rule Guidance
- Security Risk Assessment Tool
- Cyber Security Guidance
- Breach Notification Guidance
- Compliance & Enforcement

DEFINITIONS

The HIPAA Rules include many terms that have specific meanings. To understand the HIPAA Rules, refer back to these key definitions as you use the toolkit.

Availability -- The ePHI is accessible and useable upon demand by an authorized person.

Business associate – A person or organization that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI. This could include, for example, a third-party administrator or broker/consultant for a health plan. Prior to disclosing any PHI, the covered entity and business associate must enter into a written business associate agreement.

Confidentiality – The ePHI is not made available or disclosed to unauthorized people or processes.

Covered entity – A health plan, health care clearinghouse or health care provider that transmits PHI electronically. A self-funded health plan with fewer than 50 participants that is administered by the sponsoring employer is exempt from the HIPAA Rules.

Designated record set – A group of records maintained by or for a covered entity that includes the:

- Medical records and billing records about individuals maintained by or for a covered health care provider;
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals.

Electronic PHI (ePHI) – PHI that a covered entity (or business associate) creates, receives, maintains or transmits in electronic media.

HHS – The Department of Health and Human Services (HHS), the federal agency that is responsible for implementing and enforcing the HIPAA Rules.

"Hands-off" PHI – A fully insured health plan is hands-off PHI if the PHI it creates or receives from the health insurance issuer is limited to enrollment information, summary health information and information that is released pursuant to a HIPAA authorization. In this situation, most of the HIPAA compliance obligations fall on the health insurance issuer, and not on the employer-sponsored group health plan.

"Hands-on" PHI – A fully insured health plan is hands-on PHI if it creates or receives PHI from the issuer other than enrollment information, summary health information and information that is released pursuant to a HIPAA authorization. Health plans that are hands-on PHI will have significant responsibilities under the HIPAA Rules with respect to the PHI.

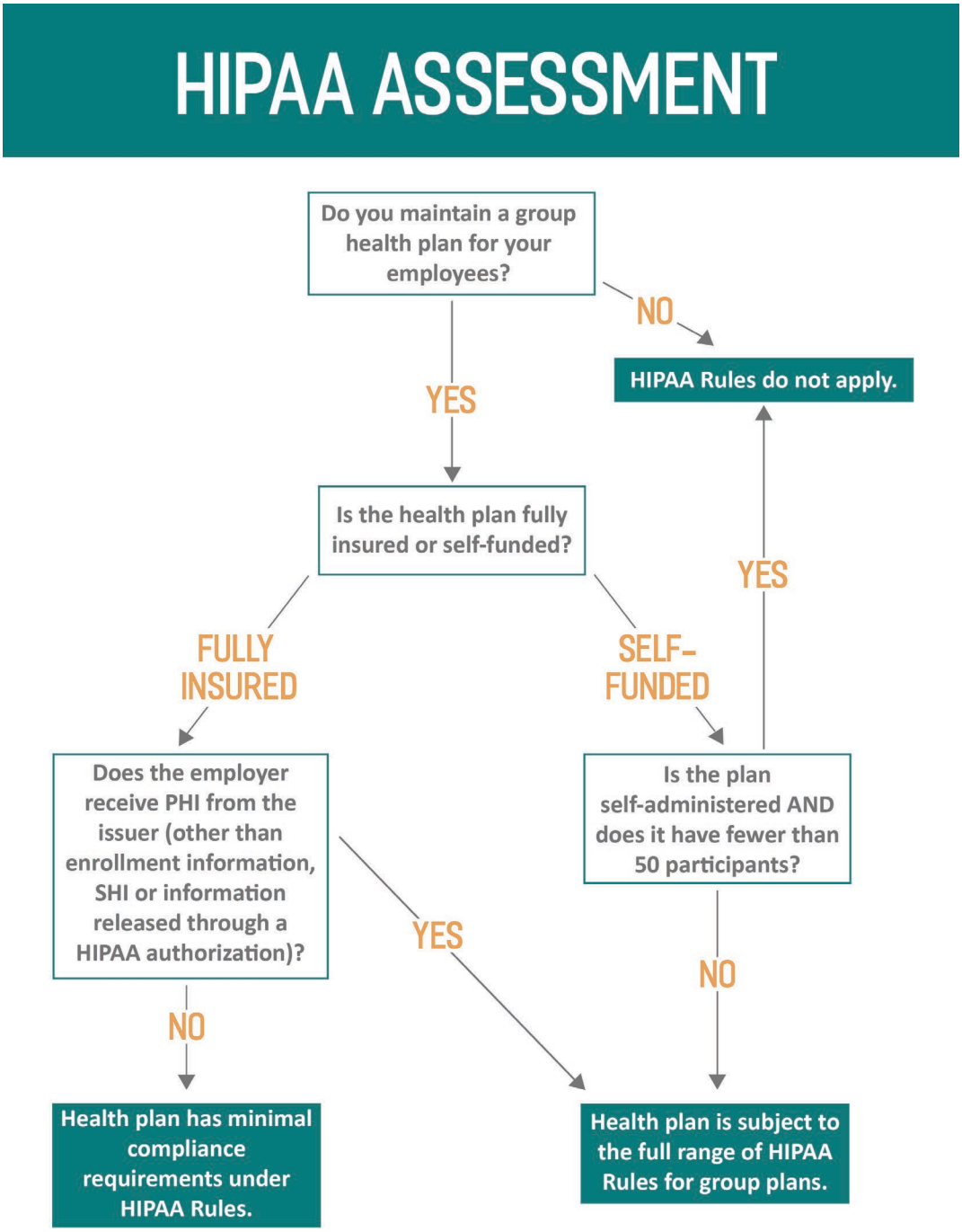
Integrity – The ePHI has not been altered or destroyed in an unauthorized manner.

Protected health information (PHI) – Individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity (or a business associate) and relates to the past, present, or future physical or mental health condition of an identified individual. Employment records are not considered PHI.

Summary health information (SHI) – Information that summarizes claims history, claims expenses or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five-digit ZIP codes.

HIPAA ASSESSMENT

To assess how the HIPAA Rules may apply to an employer-sponsored group health plan, employers should review their group health plans and their access to PHI. The following flowchart depicts these steps:



HIPAA COMPLIANCE CHECKLISTS

An employer is generally not subject to the HIPAA Rules when it performs employment-related functions, such as administering employee leaves of absence or fitness-for-duty requirements. However, the HIPAA Rules indirectly regulate employers in their role as health plan sponsors. When an employer receives PHI from its group health plan for plan administrative functions, the employer must agree to comply with certain requirements of the HIPAA Rules.

Employers should assess their group health plans to determine if the HIPAA Rules apply and, if so, to what extent. A **HIPAA assessment flowchart** is provided as part of this toolkit to help employers with this process. Also, key concepts and action items are explained throughout this toolkit. After performing a HIPAA assessment, employers should refer to the HIPAA checklist below that is applicable to them.

HIPAA CHECKLISTS	
Type of Health Plan	**Key Compliance Steps**
Fully Insured Health Plan – "Hands-off" PHI	✓ Establish a privacy policy prohibiting retaliation and waiver of rights. ✓ Perform a risk analysis regarding any ePHI that the group health plan creates or receives. ✓ Adopt appropriate administrative, technical and physical safeguards for the ePHI *(these requirements are scalable)*. ✓ Designate a security official. ✓ Adopt a breach notification policy. See the sample HIPAA policies for fully insured health plans that are hands-off PHI.
Fully Insured Health Plan – "Hands-on" PHI	✓ Implement policies and procedures that address the Privacy Rule's requirements, taking into account the health plan's size and types of activities involving PHI. ✓ Designate a privacy officer and a security official. ✓ Train workforce members on HIPAA policies and procedures. ✓ Adopt a sanctions policy for employees who fail to comply with applicable HIPAA requirements.

HIPAA CHECKLISTS	
Type of Health Plan	**Key Compliance Steps**
	✓ Implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI. ✓ Amend the health plan documents to impose restrictions on the employer's use and disclosure of PHI. ✓ Maintain a Privacy Notice (must be provided upon request). ✓ Do not use PHI from the health plan in any employment-related action or decision or in connection with any other benefit plan. ✓ Comply with individual rights' requirements. ✓ Enter into business associate agreements, as necessary. ✓ Perform a risk analysis regarding any ePHI that the group health plan creates or receives. ✓ Adopt appropriate administrative, technical and physical safeguards for ePHI (*these requirements are scalable*). ✓ Adopt a breach notification policy. ✓ Maintain HIPAA documentation for at least six years. See the sample HIPAA policies for fully insured health plans that are hands-on PHI and self-insured health plans.
Self-insured Health Plan ***Self-insured health plans with fewer than 50 participants are exempt from the HIPAA Rules if***	✓ Implement policies and procedures that address the Privacy Rule's requirements, taking into account the health plan's size and types of activities involving PHI. ✓ Designate a privacy officer and a security official. ✓ Train workforce members on HIPAA policies and procedures. ✓ Adopt a sanctions policy for employees who fail to comply with applicable HIPAA requirements.

HIPAA CHECKLISTS	
Type of Health Plan	**Key Compliance Steps**
they are self-administered.	✓ Implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI. ✓ Amend the health plan documents to impose restrictions on the employer's use and disclosure of PHI. ✓ Provide a Privacy Notice. ✓ Do not use PHI from the health plan in any employment-related action or decision or in connection with any other benefit plan. ✓ Comply with individual rights' requirements. ✓ Enter into business associate agreements, as necessary. ✓ Perform a risk analysis regarding any ePHI that the group health plan creates or receives. ✓ Adopt appropriate administrative, technical and physical safeguards for ePHI (*these requirements are scalable*). ✓ Adopt a breach notification policy. ✓ Maintain HIPAA documentation for at least six years. See the sample HIPAA policies for self-insured health plans and fully insured health plans that are hands-on PHI.

BASIC CONCEPTS

WHO IS SUBJECT TO THE HIPAA RULES?

The HIPAA Rules apply to **covered entities**. Covered entities include:

- Health plans
- Health care clearinghouses
- Most health care providers

The HIPAA Rules also apply to other entities that perform functions or activities on behalf of a covered entity when those services involve access to, or the use or disclosure of, PHI. These entities are called **business associates**.

Impact on Employers

An employer is not a covered entity under the HIPAA Rules. This means that an employer is generally not subject to the HIPAA Rules when it performs employment-related functions, such as administering employee leaves of absence or fitness-for-duty requirements. However, the HIPAA Rules **indirectly regulate employers in their role as health plan sponsors**. Although an employer and its health plan are separate legal entities, the HIPAA Rules recognize that employers often perform administrative functions on behalf of their health plans that involve PHI. When an employer receives PHI from its group health plan for plan administrative functions, the employer must agree to comply with certain requirements of the HIPAA Rules.

The impact of the HIPAA Rules on employers mainly depends on whether the health plan is insured or self-funded and, if the health plan is insured, whether the employer has access to PHI for plan administration purposes.

Covered Entities

Health Plans

In general, **any individual or group plan that provides or pays the cost of health care** is a covered entity subject to the HIPAA Rules. Health insurance issuers are also considered health plans subject to the HIPAA Rules.

There is a **special exemption for certain small, self-funded health plans**. Under this exemption, a self-funded health plan with **fewer than 50 eligible employees** that is administered by the employer that sponsors the plan is exempt from the HIPAA Rules. This exemption may apply to group medical plans, health reimbursement arrangements (HRAs) or health flexible spending accounts (FSAs) that satisfy the requirements for the exemption.

The following chart provides examples of common employee benefits provided by employers and indicates whether the benefits are health plans that are generally subject to the HIPAA Rules. If an employee benefit is not subject to the HIPAA Rules (for example, a disability insurance program), this means that information received in connection with the benefit is not PHI and is not subject to the HIPAA Rules' requirements.

Type of Employee Benefit	Subject to HIPAA Rules?
Group medical plans (fully insured or self-funded)	Yes
Dental and vision plans	Yes
Prescription drug plans	Yes
FSAs	Yes
Dependent care FSA	No
Adoption assistance FSA	No
HRAs	Yes
Health savings accounts (HSAs)	No, but the high deductible health plans (HDHPs) offered with HSAs are subject to the HIPAA Rules
Disease-specific policies, such as cancer policies	Yes, if they provide coverage for medical care
Employee assistance programs (EAPs)	Depends on the EAP's benefits—EAPs that provide medical care are subject to the HIPAA Rules
Wellness plans	Depends on wellness plan's benefits—wellness plans that provide medical care are subject to the HIPAA Rules
Life insurance	No
Disability insurance	No
Section 125 premium-only plans	No
Workers' compensation insurance	No
Retirement plans	No

Health Care Clearinghouse

A health care clearinghouse is a public or private entity that processes another entity's health care transactions from a standard format to a nonstandard format (or vice versa). In many cases, health care clearinghouses will receive individually identifiable health information when they provide services to a health plan or health care provider as a business associate. Health care clearinghouses may include, for example, repricing companies, value-added networks, billing services or community health management information systems.

Health Care Providers

Every health care provider, regardless of size, that electronically transmits any health information in connection with a HIPAA-covered transaction is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests and other transactions for which HHS has established standards under HIPAA. Covered health care providers may include, for example, chiropractors, medical clinics, dentists, doctors, nursing homes, pharmacies and hospitals.

Business Associates

A business associate is a person or organization (other than an employee of a covered entity) that performs certain functions on behalf of, or provides certain services to, a covered entity that involves access to PHI. In general, a business associate means a third party (including a subcontractor) that:

- Creates, receives, maintains or transmits PHI on behalf of the covered entity for a HIPAA-regulated activity or function, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and repricing; or
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services for the covered entity where the provision of the service involves the disclosure of PHI from the covered entity (or from another business associate of the covered entity) to the service provider.

Examples of Business Associates:

- Third-party administrators (TPAs)
- Pharmacy benefit managers (PBMs)
- Attorneys or auditors who use PHI in performing their services
- Health plan consultants or brokers

If a covered entity uses a business associate, there must be a written agreement between the parties, called a **business associate agreement**, that requires the business associate to comply with certain requirements under the HIPAA Rules. A sample business associate agreement is provided in this toolkit.

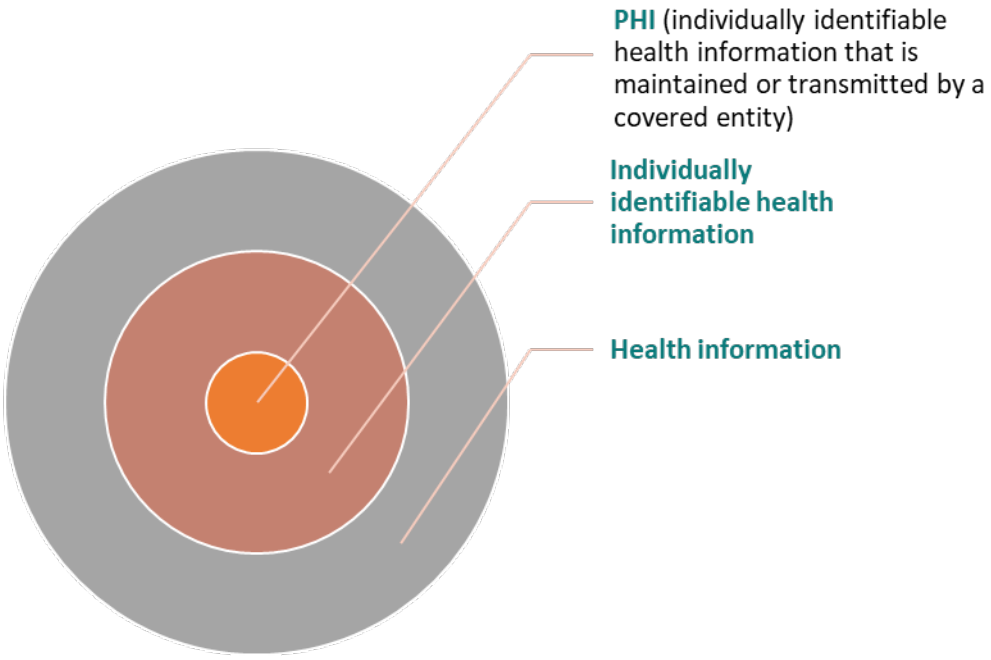
WHAT INFORMATION IS PROTECTED?

PHI

The HIPAA Rules protect **individually identifiable health information**, called PHI, that is **held or transmitted by a covered entity or its business associate**. PHI includes information that relates to any of the following:

- The past, present, or future physical or mental health or condition;
- The provision of health care to an individual; or
- The past, present or future payment for the provision of health care to the individual.

The HIPAA Privacy Rule applies to PHI in any form or media—written, verbal, electronic or in any other medium. The Security Rule's requirements, however, only apply to ePHI.



PHI does not include employment records held by an employer. These records may include, for example, files or records related to occupational injury, disability insurance eligibility, leave requests, drug screenings, workplace medical surveillance and fitness-for-duty tests. Other laws, such as the federal Americans with Disabilities Act or state privacy laws, may impose confidentiality or privacy requirements on the information.

De-identified Health Information

De-identified health information is not governed by the HIPAA Rules because it is no longer individually identifiable. Covered entities may freely use and disclose de-identified information without taking into account the HIPAA Rules. There are two different methods that may be used to de-identify health information.

Statistical Method

Under the statistical method, a person with appropriate knowledge and experience applying generally applicable statistical and scientific principles and methods for rendering information not individually identifiable makes a determination that the risk is very small that the information could be used, either by itself or in combination with other

available information, by anticipated recipients to identify the subject of the information. The covered entity must document the analysis and results that justify the determination.

Safe Harbor Method

Under the safe harbor method, information is presumed to be de-identified if a covered entity:

- Has no actual knowledge that the information could be used to identify the subject of the information (alone or in combination with other information); and
- Removes 18 specific identifiers from the information. The 18 identifiers that must be removed are:
    1. Names;
    2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code and their equivalent geocodes, except for the initial three digits of a ZIP code if, according to the current publicly available data from the Bureau of Census, (1) the geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people, and (2) the initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000;
    3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age;
    4. Telephone numbers;
    5. Fax numbers;
    6. Email addresses;
    7. Social Security numbers;
    8. Medical record numbers;
    9. Health plan beneficiary numbers;
    10. Account numbers;
    11. Certificate/license numbers;
    12. Vehicle identifiers and serial numbers, including license plate numbers;
    13. Device identifiers and serial numbers;
    14. Web URLs;
    15. IP addresses;
    16. Biometric identifiers, including finger and voice prints;
    17. Full-face photographic images and any comparable images; and
    18. Any other unique identifying number, characteristic or code.

PRIVACY REQUIREMENTS

The HIPAA Privacy Rule requires covered entities to comply with national standards for the protection of PHI. The Privacy Rule includes the following three main protections for PHI:

Use and Disclosure Rules	The Privacy Rule limits when an individual's PHI may be used or disclosed by covered entities. As a general rule, a covered entity may not use or disclose an individual's PHI except: (1) as required or permitted by the Privacy Rule; or (2) subject to the individual's written authorization.
Individual Rights	Covered health care providers and health plans must provide individuals with detailed written information that explains their privacy rights and how their information will be used. Individuals also have the right to: • Access their own health records and request corrections; • Request restrictions on the uses and disclosures of their PHI, including that communications containing PHI be sent to an alternate location; and • Obtain documentation of certain disclosures of their PHI.
Administrative Safeguards	Covered entities must develop written privacy procedures and implement appropriate safeguards. For example, covered entities must designate a privacy officer, train employees on privacy requirements and establish a system for receiving complaints. Covered entities must also refrain from intimidating or retaliatory acts, and they cannot require a waiver of HIPAA privacy rights.

Special Exception for Fully Insured Health Plans

Employers that sponsor fully insured health plans and are hands-off PHI have minimal compliance obligations under the HIPAA Privacy Rules.

USE AND DISCLOSURE RULES

The Privacy Rule restricts when covered entities may use or disclose an individual's PHI. As a general rule, covered entities may only use or disclose an individual's PHI when:

- ✓ The disclosure is required or permitted by the Privacy Rule; or
- ✓ The individual authorizes the disclosure in writing.

Employers that sponsor group health plans are also subject to these use and disclosure rules if they have access to PHI.

New Final Rule on Reproductive Health Care Privacy

On April 26, 2024, HHS issued a final rule that strengthens the HIPAA Privacy Rule by **prohibiting the disclosure of PHI related to lawful reproductive health care in certain situations**. Beginning **Dec. 23, 2024**, the final rule prohibits covered entities and business associates from using or disclosing PHI for the criminal, civil or administrative investigation of (or proceeding against) any person in connection with seeking, obtaining, providing or facilitating reproductive health care where such health care is lawful under the circumstances in which it is provided. It also prohibits the identification of any person for the purpose of initiating such an investigation or proceeding.

In certain circumstances, covered entities and business associates that receive requests for PHI potentially related to reproductive health care must obtain a **signed attestation** that the use or disclosure is not for a prohibited purpose. HHS has provided a model attestation for covered entities and business associates to use. These new requirements impact self-insured health plans and insured health plans that are "hands-on" PHI.

Required Disclosures

A covered entity must disclose PHI in only two situations:

- To individuals (or their personal representatives) when they request access to their PHI in a designated record set or when they request an accounting of disclosures of their PHI; and
- To HHS when it is investigating the covered entity's compliance with the HIPAA Rules.

Permitted Disclosures

A covered entity is permitted, but not required, to use and disclose PHI, without an individual's authorization, in certain situations, including the following:

- ***To the individual*** – A covered entity may disclose PHI to the individual who is the subject of the information.
- ***Public policy purposes*** – A covered entity may use or disclose PHI for specific public policy purposes, such as uses and disclosures that are required by law; for public health activities; about victims of abuse, neglect or domestic violence; for health care oversight activities; for judicial or administrative proceedings; for law enforcement purposes; necessary to avert a serious threat to health or safety; and for work-related injuries or illnesses.
- ***Treatment, payment and health care operations*** – A covered entity may use and disclose PHI for:
    - Its own treatment, payment and health care operations activities;
    - The treatment activities of any health care provider;

Minimum Necessary Rule

In general, when a covered entity uses, discloses or requests PHI, it must limit its use, disclosure or request to the **minimum necessary** amount of information to accomplish the intended purpose.

- The payment activities of another covered entity or any health care provider; or
- The health care operations of another covered entity if both covered entities has (or had) a relationship with the individual, the PHI pertains to the relationship and the disclosure involves quality or competency assessment activities or fraud and abuse detection and compliance activities.

The Privacy Rule provides special protections to certain types of health information that are particularly sensitive and often involve highly personal health decisions. These types of health information include psychotherapy notes and, effective Dec. 23, 2024, reproductive health care.

Authorized Disclosures

A covered entity **must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule**. In general, a health plan may not condition payment, enrollment or benefits eligibility on an individual granting an authorization, except in limited circumstances.

An authorization must be written in specific terms. It may allow use and disclosure of PHI by the covered entity seeking the authorization or by a third party. The following information must be contained—in plain language—in HIPAA authorizations:

- A description of the information to be used or disclosed;
- The name or other specific identification of the person who is authorized to release the PHI;
- The name or other specific identification of the person who is authorized to receive the PHI;
- A description of the purpose of the requested use or disclosure (for example, at the request of the individual);
- An expiration date or event;
- A statement that the individual has a right to revoke an authorization in writing and an explanation of the procedures for revocation;
- An explanation of the covered entity's ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the receipt of an authorization;
- A statement that informs the individual that the information used or disclosed pursuant to the authorization is subject to re-disclosure by the recipient and may no longer be protected by the HIPAA Privacy Rule; and
- The individual's signature and date of signature.

Compliance Tip for Employers

Some common employer functions that involve employees' medical information may require HIPAA authorizations, such as obtaining drug testing results and fitness-for-duty information from health care providers. A HIPAA authorization is also required in order for an employer to help an employee with a claim dispute involving the health insurance issuer. Medical information that is directly provided by the employee to the employer is generally not subject to the HIPAA Rules. However, a valid HIPAA authorization is needed to obtain employees' medical or claim information directly from covered entities (such as health care providers or health insurance issuers).

Other Disclosures

Disclosures to Plan Sponsors

A group health plan (and the health insurance issuer for a fully insured plan) may disclose the following PHI to the employer sponsoring the plan:

- ✓ Plan **enrollment or disenrollment** information;
- ✓ If requested by the plan sponsor, **summary health information** for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend or terminate the group health plan; and
- ✓ PHI of the group health plan's enrollees for the plan sponsor to perform **plan administration functions**.

If a plan sponsor has access to PHI other than summary health information and enrollment and disenrollment information, the plan must receive certification from the plan sponsor that the **group health plan document has been amended** to impose restrictions on the plan sponsor's use and disclosure of the PHI. These restrictions must include the representation that the plan sponsor will not use or disclose the PHI for any employment-related action or decision or in connection with any other benefit plan.

A sample plan amendment and a sample certification are provided in this toolkit.

Disclosures to Business Associates

The HIPAA Rules allow a covered entity to share PHI with a business associate if the covered entity receives satisfactory assurances from the business associate—through a **business associate agreement**—that it will appropriately handle and safeguard PHI. A business associate may use or disclose PHI only as permitted or required by its business associate agreement or as required by law. In general, a business associate is prohibited from using or disclosing PHI in a manner that would violate the HIPAA Privacy Rule if done by the covered entity.

The business associate agreement must establish the permitted and required uses and disclosures of PHI by the business associate. The business associate agreement must also require the business associate to:

- Not use or further disclose the PHI other than as permitted or required by the contract or as required by law;

- Use appropriate safeguards to prevent improper use or disclosure of the PHI;
- Report to the covered entity any known use or disclosure of PHI not permitted by the contract or any breach of unsecured PHI;
- Ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions that apply to the business associate;
- Make PHI available, including for amendment, to individuals as required by the HIPAA Rules;
- Maintain an accounting of disclosures, made during the last six years, and make the accounting available upon request; and
- Make its internal practices, books and records relating to use and disclosure of PHI available to HHS.

> ***Enforcement Example: No Business Associate Agreement***
>
> In April 2017, HHS entered into a HIPAA settlement with a small health care provider following an investigation of a business associate. Neither the health care provider nor the business associate could produce a signed business associate agreement. Based on this HIPAA violation, the health care provider agreed to pay HHS **$31,000** to settle the investigation.

The business associate contract must also allow the covered entity to terminate the contract in the event of a material breach. At termination, the business associate must be required to destroy or return all PHI, if feasible, or extend the limitations on use and disclosure beyond termination of the contract.

A sample business associate agreement is provided in this toolkit.

INDIVIDUAL RIGHTS

Notice of Privacy Practices

The HIPAA Privacy Rule requires covered entities to provide a **Notice of Privacy Practices** to each individual who is the subject of PHI. The Privacy Notice for a health plan must be written in plain language and must:

- Explain how the health plan may use and disclose an individual's PHI;
- Describe the individual's rights with respect to their PHI; and
- Summarize the health plan's legal duties with respect to the PHI.

There are a number of specific provisions that must be incorporated into the Privacy Notice, such as details regarding how individuals may exercise their rights with respect to PHI. A typical Privacy Notice is multiple pages long due to the numerous content requirements.

The Privacy Notice requirements for a health plan vary depending on whether the plan is self-insured or fully insured, and, if the plan is fully insured, whether the plan sponsor has access to PHI for plan administration purposes. A self-insured plan must always issue its own Privacy Notice, while a fully insured plan is only required to maintain its own Privacy Notice if the employer has access to PHI for plan administration functions.

UPDATE: HHS' final rule on reproductive health care privacy requires covered entities, including health plans, to update their Privacy Notices to describe the new privacy rights for reproductive health care and provide examples of the new

disclosure restrictions. It also requires Privacy Notices to explain that PHI disclosed pursuant to the Privacy Rule may be subject to redisclosure and is no longer protected. In addition, covered entities that handle certain substance use disorder patient records must update their Privacy Notices to describe new privacy protections for these records. The deadline for covered entities to update their Privacy Notices for these changes is **Feb. 16, 2026**. It is expected that HHS will update its model Privacy Notices to incorporate the new requirements.

Special Rules for Fully Insured Health Plans

The plan sponsor of a fully insured health plan has limited responsibilities with respect to the Privacy Notices. The extent of its limited responsibilities depends on whether the plan sponsor has access to PHI for plan administration functions.

- ✓ If the sponsor of a fully insured plan is hands-on PHI, it is required to maintain a Privacy Notice and to provide the notice upon request.
- ✓ If the sponsor of a fully insured plan is hands-off PHI, it is not required to maintain or provide a Privacy Notice.

Delivery Requirements

At least once every three years, self-insured health plans must provide the Privacy Notice, or notify participants that the notice is available with instructions for how to obtain a copy. In addition, self-insured health plans must provide the Privacy Notice in the following circumstances:

- To new enrollees at the time of enrollment;
- Within 60 days of a material change to the notice; and
- Any time upon a participant's request.

If a health plan sends out a revised notice (for example, following a material change to the notice), it will reset the three-year notice requirement.

A health plan must provide the Privacy Notice to individuals covered by the plan. If the health plan provides the Privacy Notice to a covered employee, the plan is not required to provide a separate notice for dependents (for example, a spouse or child) covered through the employee.

The Privacy Notice must be actually delivered to participants. Merely posting the Privacy Notice on a website or on a bulletin board in the workplace is not sufficient. The Privacy Notice may be provided electronically via email to participants who have agreed to receive an electronic notice. The health plan must provide a participant with a paper copy of the Privacy Notice if it discovers that the electronic delivery has failed.

In general, the Privacy Notice may be provided with other plan documents. It does not need to be provided as a stand-alone document. For example, a health plan could provide the Privacy Notice with the plan's enrollment

materials or with the summary plan description (SPD). However, the Privacy Notice may not be combined in the same document as a HIPAA authorization.

If a health plan maintains a website about the plan's services or benefits, the Privacy Notice must be posted on the website and must be electronically available through the website.

Model Privacy Notices

HHS has developed model Privacy Notices that health plans may customize and use. There are three designs for the model Privacy Notice for health plans—a booklet version, a full-page version and a layered version. Every design has the same language, although the layered notice includes an additional first page that summarizes key privacy rights, choices, uses and disclosures.

Each design is in a fillable Adobe PDF format and has some areas that can be customized for each health plan. More information on customizing the notice and best practices is available in the Health Plan Instructions and Questions and Instructions for using the Model Notices. For additional flexibility, HHS also maintains a text-only version of the model Privacy Notice.

Other Individual Rights

The Privacy Rule requires covered entities to provide individuals with the following rights with respect to their PHI:

Individual Right	Description
Right to access PHI	Except in certain circumstances, individuals have the right to inspect and obtain a copy of their PHI in a designated record set that is maintained by or for a covered entity.
Right to amend or correct PHI	Individuals have the right to request that covered entities amend or correct their PHI in a designated record set when that information is inaccurate or incomplete. Covered entities must comply with these requests, subject to certain limitations.
Right to obtain an accounting of disclosures	Individuals have a right to an accounting of certain disclosures of their PHI by a covered entity. Many common group health plan disclosures (such as disclosures for payment and health care operations) are exempted from this accounting requirement.
Right to request restrictions on uses and disclosures	Individuals have the right to request that a covered entity restrict its use or disclosure of PHI with respect to: (1) treatment, payment or health care operations; or (2) other people involved in the individual's care. In general, a covered entity is not required to agree to requests for restrictions.
Right to request alternative communications	A health plan must permit individuals to request to receive communications of PHI by alternative means or at alternative locations. A health plan must accommodate

reasonable requests if the individual clearly indicates that the disclosure of all or part of the PHI could endanger the individual.

Fully insured health plans that are hands-off PHI are not subject to these individual rights requirements. Rather, individuals who are enrolled in these health plans would exercise their privacy rights through the health insurance issuer.

ADMINISTRATIVE REQUIREMENTS

In general, the HIPAA Privacy Rule requires a health plan to comply with the following administrative requirements:

- **Implement reasonably designed policies and procedures** that address the Privacy Rule's requirements and are designed to ensure compliance with those requirements, taking into account the health plan's size and types of activities that involve PHI;
- Designate a **privacy officer** responsible for the development and implementation of the health plan's privacy policies and procedures;
- Designate a **contact person** (who may also be the privacy official) responsible for receiving privacy complaints and providing information about privacy practices;
- **Train** all members of its workforce on the its policies and procedures with respect to PHI, as necessary and appropriate for those individuals to carry out their job functions;
- Put in place appropriate **administrative, technical and physical safeguards** to protect the privacy of PHI;
- Provide a **complaint process** for individuals regarding the health plan's privacy policies and procedures and **document any privacy complaints** that it receives;
- Establish and apply **appropriate sanctions** against members of its workforce who fail to comply with the health plan's privacy policies and procedures and **document any sanctions** that are applied;
- **Mitigate, to the extent possible, the harmful effect** of any violation of its privacy policies or procedures;
- **Refrain from intimidating or taking retaliatory action** against any individual who exercises their individual privacy rights or files a privacy complaint;
- Do not require individuals to **waive their privacy rights** as a condition of enrollment in the plan, eligibility for benefits or payment;

Exception for Fully Insured Health Plans

Fully insured group health plans that are "hands off" PHI are not subject to most of the Privacy Rule's administrative requirements. These health plans are only required to comply with the ban on retaliatory acts and waiver of individual rights.

- ✓ Provide a **Privacy Notice** to plan participants (special exception applies for fully insured health plans);
- ✓ Require all business associates to enter into **business associate agreements** with the health plan;
- ✓ Confirm that the **plan document has been amended**, as required by the Privacy Rule;
- ✓ Do not use PHI from the health plan in any **employment-related action or decision** or in connection with any **other benefit plan**; and
- ✓ Maintain the plan's privacy policies and documentation required by the Privacy Rule for **at least six years**.

SECURITY REQUIREMENTS

The HIPAA Security Rule establishes national standards for securing individuals' ePHI. These standards require covered entities to analyze the risks and vulnerabilities of the confidentiality, integrity and availability of their ePHI. The risk assessment process helps covered entities implement reasonable and appropriate administrative, physical and technical safeguards to protect their ePHI.

Impact on Health Plans

In general, sponsors of self-insured and fully insured group health plans should conduct risk assessments and implement appropriate safeguards to protect their ePHI. Unlike the Privacy Rule, the Security Rule does not contain a special exception for fully insured plans that do not have access to PHI for plan administration purposes. However, fully insured health plans that do not handle ePHI will have fewer obligations under the Security Rule due to their hands-off approach to PHI.

ELECTRONIC PHI

The Security Rule only applies to ePHI—it does not apply to PHI that is in paper or written form, and it does not apply to electronic personal information that is not PHI.

Electronic PHI is PHI that is transmitted by, or maintained in, electronic media. This includes PHI in computers, devices that are used with computers (such as disks and drives), and smartphones. It also includes PHI that is sent via email or in any manner using the internet.

The Security Rule's requirements apply even when the ePHI is located on a device that is not owned by the covered entity (for example, an employee's smartphone) or is accessed outside of the covered entity's physical location (for example, on a home computer or on a laptop outside of work). HHS has cautioned that covered entities should be extremely careful about allowing off-site use of, or access to, ePHI due to security risks involved.

SECURITY REQUIREMENTS

The HIPAA Security Rule requires covered entities to maintain **reasonable and appropriate administrative, technical and physical safeguards** for protecting ePHI. Each covered entity must analyze the risks to ePHI in its environment and create solutions appropriate for its own situation. What is reasonable and appropriate depends on the nature of the entity's business, as well as its size, complexity and resources. Specifically, a covered entity must:

- ✓ Ensure the confidentiality, integrity and availability of all ePHI it creates, receives, maintains or transmits;
- ✓ Identify and protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
- ✓ Protect against reasonably anticipated use or disclosure of ePHI that is not permitted or required under the HIPAA Privacy Rule; and

✓ Ensure its workforce complies with the procedures implemented to comply with the HIPAA Security Rule.

Risk Assessment

According to HHS, performing a risk assessment is a **crucial first step** to comply with the Security Rule. A risk assessment helps an organization establish appropriate administrative, physical and technical safeguards for its ePHI. It directs what reasonable steps a covered entity or business associate should take to protect the ePHI it creates, transmits, receives or maintains.

There are numerous methods of performing a risk assessment, and there is no single method or best practice that guarantees compliance with the Security Rule. However, most risk analysis processes have common steps. The following are examples of common risk analysis steps:

Elements for Risk Assessment	
Identify the scope of analysis	The scope should include the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that a covered entity creates, receives, maintains or transmits.
Gather data	Gather relevant data on ePHI and identify where ePHI is stored, received, maintained or transmitted.
Identify potential threats and vulnerabilities	Identify and document potential threats and vulnerabilities to the confidentiality, availability and integrity of ePHI.
Assess current security measures	Analyze current security measures implemented to minimize or eliminate risks to ePHI.
Determine the likelihood of threat occurrence	Use information gathered from the previous steps to assess: (1) the likelihood that a threat will trigger or exploit a specific vulnerability; and (2) the resulting impact on the health plan.
Determine the potential impact of threat occurrence	Measure the impact of a threat occurring, such as the unauthorized access to or disclosure of ePHI, permanent loss of corruption of ePHI, or temporary loss or unavailability of ePHI.
Determine risk level	Determine the level of risk to ePHI (based on the likelihood of threat occurrence and the potential impact of threat occurrence).
Identify security measures and finalize documentation	Identify security measures that can be used to reduce risk to a reasonable and appropriate level and document the risk analysis.

Also, to better understand the risk analysis and management processes, covered entities should be familiar with the following terms:

- **Vulnerability** means a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of security policy.
- **Threat** means the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. Threats may be grouped into the following categories:
    - **Natural threats**, such as floods, earthquakes, tornadoes and landslides;
    - **Human threats**, including intentional (for example, network and computer-based attacks, malicious software upload and unauthorized access) and unintentional (for example, inadvertent data entry or deletion) actions; and
    - **Environmental threats**, such as power failures, pollution, chemicals and liquid leakage.
- **Risk** means the net impact considering the probability that a particular threat will exercise a particular vulnerability and the resulting impact if this should occur.

Security Standards

The security standards are divided into the following three categories:

Each type of safeguard has certain standards and implementation specifications associated with it.

- ✓ **Administrative safeguards** – These are the administrative actions, policies and procedures to prevent, detect, contain and correct security violations.
- ✓ **Physical safeguards** – These are the physical measures, policies and procedures to protect electronic systems and related building and equipment from natural and environmental hazards and unauthorized intrusion.
- ✓ **Technical safeguards** – These safeguards are the technology and procedures that protect ePHI and control access to it.

The **standards and implementation specifications** for each type of safeguard are listed in the Security Standards Matrix below. The Security Rule allows covered entities some flexibility in determining how to implement the standards and implementation specifications, including choosing which technology it will employ in order to achieve the required security standards. In deciding how to implement security measures, a covered entity is permitted to take into account:

- ✓ Its size, complexity and capabilities;
- ✓ Its technical infrastructure, hardware and software security capabilities;
- ✓ The costs of security measures; and
- ✓ The probability and criticality of potential risks to health information.

Enforcement Example: In January 2017, the Office for Civil Rights (OCR) announced a HIPAA settlement with an insurance company regarding an impermissible disclosure of ePHI. The disclosure involved a USB data storage device containing ePHI that was stolen from the company's IT department, where the device was left without safeguards overnight. Pursuant to the settlement, the insurance company paid **$2.2 million** and implemented a corrective action plan.

However, HHS has stated that cost alone is not a justification for failing to implement a procedure.

In an effort to provide covered entities with additional flexibility, the Security Rule categorizes implementation specifications as "required" or "addressable." The "required" implementation specifications must be implemented.

The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.

POLICIES AND PROCEDURES

Covered entities are required to implement **reasonable and appropriate policies and procedures** to comply with the Security Rule's standards and implementation specifications. These policies and procedures must be documented in written form, which may be electronic. In addition, a covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of ePHI. Documentation supporting its security policies must be retained for **at least six years** from the date of its creation or the date when it was last in effect, whichever is later.

SECURITY STANDARDS MATRIX

SECURITY STANDARDS MATRIX		
Standards	**Implementation Specifications (R) = Required and (A) = Addressable**	
ADMINISTRATIVE SAFEGUARDS		
Security Management Process	Risk Analysis	(R)
	Risk Management	(R)
	Sanction Policy	(R)
	Information System Activity Review	(R)
Assigned Security Responsibility		(R)
Workforce Security	Authorization and/or Supervision	(A)
	Workforce Clearance Procedure	(A)
	Termination Procedures	(A)
Information Access Management	Isolating Health Care Clearinghouse Functions	(R)
	Access Authorization	(A)
	Access Establishment and Modification	(A)
Security Awareness and Training	Security Reminders	(A)
	Protection from Malicious Software	(A)
	Login Monitoring	(A)
	Password Management	(A)
Security Incident Procedures	Response and Reporting	(R)
Contingency Plan	Data Backup Plan	(R)
	Disaster Recovery Plan	(R)
	Emergency Mode Operation Plan	(R)
	Testing and Revision Procedures	(A)

	Applications and Data Criticality Analysis	(A)
Evaluation		(R)
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement	(R)
PHYSICAL SAFEGUARDS		
Facility Access Controls	Contingency Operations	(A)
	Facility Security Plan	(A)
	Access Control and Validation Procedures	(A)
	Maintenance Records	(A)
Workstation Use		(R)
Workstation Security		(R)
Device and Media Controls	Disposal	(R)
	Media Reuse	(R)
	Accountability	(A)
	Data Backup and Storage	(A)
TECHNICAL SAFEGUARDS		
Access Control	Unique User Identification	(R)
	Emergency Access Procedure	(R)
	Automatic Logoff	(A)
	Encryption and Destruction	(A)
Audit Controls		(R)
Integrity	Mechanism to Authenticate Electronic PHI	(A)
Person or Entity Authentication		(R)
Transmission Security	Integrity Controls	(A)
	Encryption	(A)

BREACH NOTIFICATION REQUIREMENTS

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) amended HIPAA to add breach notification requirements for unsecured PHI. The HITECH Act, and its underlying HIPAA breach notification rules, require covered entities to notify affected individuals following the discovery of a breach of unsecured PHI. Notification must also be provided to HHS and, in some cases, to the media.

BREACH OF UNSECURED PHI

The HIPAA Rules define a "breach" as the unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of the information. There are three exceptions to this definition.

1. Disclosures where the recipient of the information would not reasonably have been able to retain the information;
2. Certain unintentional acquisition, access, or use of information by employees or others acting under the authority of a covered entity or business associate; and
3. Certain inadvertent disclosures among people similarly authorized to access PHI at a business associate or covered entity.

Unsecured PHI

The breach notification requirements only apply to **unsecured PHI**. PHI is unsecured if it is not rendered unusable, unreadable or indecipherable to unauthorized individuals by a methodology specified by HHS. HHS has specified **encryption and destruction** as the methodologies for securing PHI.

An impermissible use or disclosure of PHI is **presumed to be a breach** unless the covered entity or business associate demonstrates through a **risk assessment** that there is a **low probability** that the PHI has been compromised (or one of the three exceptions to the definition of breach applies). The risk assessment must, at a minimum, take into account these factors:

- ✓ The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;
- ✓ The unauthorized person who used the PHI or to whom the disclosure was made;
- ✓ Whether the PHI was actually acquired or viewed; and
- ✓ The extent to which the risk to the PHI has been mitigated.

If an evaluation of the factors fails to demonstrate that there is a low probability that PHI has been compromised, breach notification is required.

BREACH NOTIFICATION

Notice to Individuals

If a covered entity discovers that it has experienced a breach of unsecured PHI, it must notify each individual whose unsecured PHI has been (or is reasonably believed by the covered entity to have been) accessed, acquired, used or

disclosed as a result of the breach. The notice must be provided without unreasonable delay and in no case later than **60 calendar days** after the breach is discovered.

The notice must be written in plain language and must contain the following information:

- A brief description of what happened, including the dates the breach occurred and was discovered, if known;
- A description of the types of unsecured PHI that were involved, such as names, Social Security numbers or other types of information;
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the covered entity involved is doing to investigate the breach, mitigate harm to individuals and protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, including a toll-free telephone number, an email address, website or postal address.

> ***Enforcement Example***: In January 2017, OCR announced a HIPAA settlement with a health care provider based on the untimely reporting of a breach of unsecured PHI. After receiving a breach notification report from the health care provider, OCR investigated and found that the provider failed to notify affected patients, media outlets and OCR within 60 days of the discovery. Pursuant to the settlement, the provider paid **$475,000** to OCR and implemented a corrective action plan.

In general, notice must be provided in writing, by first-class mail to the individual's last known address. Notice can be sent electronically if the individual has agreed to electronic notice. In a case that requires urgency because of possible imminent misuse of unsecured PHI, the covered entity may provide notice by telephone or other means.

Notice to HHS

Covered entities must notify HHS of a breach of unsecured PHI. However, the notification required depends on the size of the group affected.

Breaches involving fewer than 500 individuals	The covered entity must maintain a log or other documentation of the breaches. Within 60 days after the end of each calendar year, the covered entity must notify HHS of the breaches that occurred during the year.
Breaches involving 500 or more individuals	The notice must be provided at the same time as the notice to the individuals and in the manner specified on the HHS website.

Notice to the Media

If the breach of unsecured PHI involves **more than 500 residents of a state or jurisdiction**, the covered entity must notify prominent media outlets that serve that area. The notice must include the same information as a notice to an individual. It must be provided without unreasonable delay and no later than **60 calendar days** after the breach is discovered.

Business Associate Role

If a business associate discovers a breach of unsecured PHI, it must notify the covered entity of the breach. Notification must be provided without unreasonable delay and no later than 60 calendar days after the breach is discovered. The notice must include, to the extent possible, the identification of each individual whose unsecured PHI has been affected. The business associate must also give the covered entity any information necessary to notify the individual of the breach.

ADMINISTRATIVE REQUIREMENTS

Covered entities must incorporate compliance with the breach notification requirements into their HIPAA privacy policies and procedures. Covered entities and business associates have the burden of demonstrating that all notifications were provided or that an impermissible use or disclosure did not constitute a breach, and must maintain documentation to meet the burden of proof.

ENFORCEMENT

HHS' OCR is responsible for enforcing the HIPAA Privacy and Security Rules. OCR investigates complaints that individuals file, conducts compliance reviews, and performs education and outreach to encourage compliance. OCR also works with the Department of Justice regarding possible criminal violations of HIPAA.

Enforcement Data

As of July 31, 2024, OCR has received over 366,377 HIPAA complaints and has initiated over 1,191 compliance reviews. OCR has resolved 99% of these cases (363,234). In many cases involving HIPAA violations, OCR worked with the entities involved to apply corrective measures instead of imposing penalties. However, to date, OCR has settled or imposed a civil money penalty in 147 of these cases, resulting in a total dollar amount of $143,728,972 . More information regarding HIPAA enforcement is available through OCR's website.

Most of OCR's investigations are **trigged by individuals' complaints** regarding HIPAA violations or a **covered entity's breach notification reports**. OCR has investigated many different types of entities, including national pharmacy chains, major medical centers, group health plans, hospital chains and small provider offices.

OCR's most investigated compliance issues (in order of frequency):

- Impermissible uses and disclosures of PHI;
- Lack of safeguards on PHI;
- Lack of patient access to PHI;
- Lack of administrative safeguards to protect ePHI; and
- Uses or disclosures of more than the minimum necessary PHI.

HIPAA AUDITS

OCR has audited covered entities and business associates to ensure their compliance with the HIPAA Rules. According to OCR, these HIPAA audits are primarily a compliance improvement activity. However, if an audit reveals a serious compliance issue, OCR may initiate a review to investigate.

- ✓ In 2011 and 2012, OCR implemented a pilot audit program to assess the controls and processes implemented by covered entities to comply with HIPAA's requirements.
- ✓ In 2016 and 2017, OCR conducted the second phase of its HIPAA audit program. This second phase of HIPAA audits included both desk audits and onsite audits of covered entities and their business associates. On Dec. 17, 2020, OCR released its audit report for this phase of its audit program.

OCR may implement a permanent audit program in the future, depending on the availability of agency resources. According to OCR, these HIPAA audits are primarily a compliance improvement activity. However, if an audit reveals a serious compliance issue, OCR may initiate a compliance review to investigate.

CIVIL PENALTIES

OCR has the authority to assess civil penalties for violations of the HIPAA Privacy or Security Rules. The amount of the penalty depends on the type of violation involved. These penalties may not apply if the violation is corrected within 30 days of the date the person knew, or should have known, of the violation. HHS is also required to assess penalties for violations involving willful neglect and to formally investigate complaints of such violations.

These civil penalty amounts are subject to annual inflation-related increases. The penalty amounts that apply to civil penalties that are assessed on or after Oct. 6, 2023, are as follows:

Category of violation	Minimum penalty per violation	Maximum penalty per violation
Did not know	$141	$71,162
Reasonable cause	$1,424	
Willful neglect, corrected	$14,232	
Willful neglect, not corrected	$71,162	$2,134,831

CRIMINAL PENALTIES

Criminal penalties may be assessed for violations of the HIPAA Privacy and Security Rules. These penalties are $50,000 and one year in prison for knowing violations, $100,000 and five years in prison for violations committed under false pretenses, and $250,000 and 10 years in prison for offenses committed for commercial or personal gain.

AMOUNT OF PENALTIES - IMPORTANT FACTORS

The Enforcement Rule provides some guidance on the actions that constitute a single violation, but gives HHS the authority to determine the number of violations based on the nature of the covered entity's obligation to act or not act under the provision that is violated. Where a violation is continuing, a separate violation occurs each day that the covered entity is in violation of the requirements. Also, HHS must consider certain aggravating or mitigating factors when imposing civil penalties. These factors include the following:

- ✓ The nature and extent of the violation, including (but not limited to) the number of individuals affected and the time period during which the violation occurred;

- ✓ The nature and extent of the harm resulting from the violation, including whether the violation resulted in physical harm, financial harm, harm to an individual's reputation or hindered an individual's ability to obtain health care;
- ✓ The history of prior compliance with HIPAA's administrative simplification requirements, including whether the current violation is the same or similar to previous instances of noncompliance, whether and to what extent the covered entity has attempt to correct prior instances of noncompliance, how the covered entity has responded to technical compliance assistance from OCR and how the covered entity has responded to prior complaints;
- ✓ The financial condition and size of the covered entity; and
- ✓ Any other matters as justice may require.

Civil money penalties may not be imposed if HHS determines that the violation was not due to willful neglect and it is corrected within a time frame specified by HHS (that is, within 30 days). Willful neglect is defined as a conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provisions. HHS has discretion to expand the 30-day time period depending on the nature and extent of the covered entity's compliance failure.

For violations due to reasonable cause and not to willful neglect that are not corrected in a timely manner, HHS may waive civil money penalties, in whole or in part, to the extent that payment of the penalty would be excessive relative to the violation. In addition, HHS must initiate civil money penalty actions within six years from the date the alleged violation occurred.

Resolution Agreements vs. Civil Penalties

Rather than imposing civil penalties, OCR almost always resolves HIPAA violations informally with covered entities (or business associates) through resolution agreements. These agreements typically include a monetary settlement amount that is a fraction of the potential civil monetary penalties and a corrective action plan that requires the covered entity (or business associate) to fix remaining compliance issues.

SAMPLE DOCUMENTS

SAMPLE HIPAA POLICIES – Fully insured health plans that are hands-off PHI

- Sample HIPAA Privacy Policy
- Sample HIPAA Security Policy
- Sample Breach Notification Policy

SAMPLE HIPAA POLICIES – Fully insured health plans that are hands-on PHI and self-insured health plans

- Sample HIPAA Privacy Policy
- Sample HIPAA Security Policy
- Sample Breach Notification Policy

OTHER SAMPLE DOCUMENTS

- Sample health plan amendment
- Sample plan sponsor certification
- Sample business associate agreement
- Sample Notice of Privacy Practices (Privacy Notice)
- Sample notice of availability of Privacy Notice (self-insured health plans)
- Sample HIPAA Authorization
- Model HIPAA Attestation for reproductive health care privacy

Caution

These sample HIPAA policies and related documents are based on hypothetical employers and health plan designs and are provided for educational and illustrative purposes only. They will not apply to every employer's situation, and they must be customized for a specific employer's circumstances. These sample policies are not exhaustive—depending on an employer's situation, additional policies may be required. Nothing in this toolkit should be considered as legal advice, including these sample documents. Employers should work with knowledgeable benefits counsel to obtain legal advice on HIPAA compliance.

SAMPLE HIPAA POLICIES

FULLY INSURED HEALTH PLAN – NO ACCESS TO PHI

IMPORTANT – CUSTOMIZATION REQUIRED

The following are sample HIPAA policies for **fully insured health plans that are "hands-off" PHI**. These samples cannot be used "as is"—they **must be customized** for specific plan and employer information. Also, if the sample policies do not accurately reflect an employer's implementation of the HIPAA Rules, they should be customized for the employer's specific approach. We encourage all customization to take place in coordination with knowledgeable benefits counsel.

Self-insured health plans and fully insured health plans that have access to PHI should not use these sample HIPAA policies. These health plans have additional responsibilities under the HIPAA Rules.

Nothing in this toolkit should be considered as legal advice, including these sample documents. These sample documents are provided for educational and illustrative purposes only.

SAMPLE HIPAA Privacy Policy

The HIPAA Privacy Rule (45 CFR Part 160 and Part 164, subparts A and E) requires covered entities (and their business associates) to comply with national standards for the protection of protected health information (PHI). The Privacy Rule limits when an individual's PHI can be used or disclosed, gives individuals rights over their PHI and requires appropriate safeguards to protect the privacy of PHI.

INTRODUCTION

The **[Insert Group Health Plan Name]** (Health Plan) is a group health plan sponsored by **[Insert Company Name]** (Plan Sponsor). The Health Plan and Plan Sponsor intend to comply with the HIPAA Privacy Rule, to the extent its requirements are applicable to the Health Plan.

This Privacy Policy includes the Health Plan's policies and procedures for complying with applicable requirements of the HIPAA Privacy Rule. The Plan Sponsor reserves the right to amend or change this Privacy Policy at any time (including retroactively) without notice, except to the extent notice is required under the HIPAA Privacy Rule.

This Privacy Policy does not create any third-party rights (including, but not limited to, rights of Health Plan participants, covered dependents and business associates). This policy is a guideline for compliance with the HIPAA Privacy Rule and will not be binding on the Plan Sponsor to the extent it establishes requirements and obligations beyond those required by the HIPAA Privacy Rule. This policy does not address requirements under other federal laws or state laws. To the extent this policy conflicts with the applicable requirements of the HIPAA Privacy Rule, the Privacy Rule shall govern.

Exception For Insured Group Health Plans

The Health Plan provides benefits solely through an insurance contract with a health insurance issuer or health maintenance organization (Issuer). Pursuant to the HIPAA Privacy Rule (45 CFR § 164.530(k)), the Health Plan and Plan Sponsor do not create or receive PHI, except for:

- Summary health information (as defined under 45 CFR § 164.504(a));
- Information on whether an individual is participating in the Health Plan, or is enrolled in or has disenrolled from an Issuer; or
- PHI that is provided to the Health Plan or Plan Sponsor pursuant to and in compliance with a valid HIPAA authorization under 45 CFR § 164.508.

Because the Health Plan and Plan Sponsor comply with the limitations on creating and receiving PHI as described above, the Health Plan is not subject to most of the HIPAA Privacy Rule's requirements for health plans. For example, due to its limited access to PHI, the Health Plan is NOT required to:

- Designate a privacy officer;
- Train workforce members on the HIPAA Privacy Rule;
- Implement administrative, technical and physical safeguards to protect the privacy of PHI;
- Implement a sanctions policy for workforce members who violate HIPAA privacy policies; or
- Provide or maintain a Notice of Privacy Practices (Privacy Notice).

Most of these requirements, however, do apply to the Issuer. For example, the Issuer will provide a Privacy Notice to covered employees.

DEFINITIONS

Except as otherwise described in this policy, all terms used shall have the definition given to them by the HIPAA Privacy and Security Rules, as applicable.

- *Protected health information (PHI)* – Individually identifiable health information that is maintained or transmitted by a covered entity in any form (electronic, written or oral), subject to certain exclusions.
- *Summary health information* – Information, which may be individually identifiable, that summarizes the claims history, claims expenses or type of claims experienced by individuals for whom the plan sponsor has provided health benefits under a group health plan, and that is stripped of all individual identifiers other than five digit ZIP code.

COMPLIANCE REQUIREMENTS

No Intimidation or Retaliatory Acts

The Health Plan (and the Plan Sponsor) will not threaten, intimidate, coerce, harass, discriminate against or take any other retaliatory action against any individual for:

- Exercising their rights under the HIPAA Rules;
- Participating in any process provided under the HIPAA Rules, including the filing of a complaint;
- Testifying, assisting or participating in an investigation, compliance review, proceeding or hearing under the HIPAA Rules; or
- Opposing any act or practice that is unlawful under HIPAA, provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Rule.

No Waiver of Rights

The Health Plan may not require individuals to waive their rights under the HIPAA Rules as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

SAMPLE HIPAA Security Policy

The HIPAA Security Rule (45 CFR Part 160 and Part 164, subparts A and C) establishes national standards to protect individuals' electronic protected health information (ePHI) that is created, received, used or maintained by a covered entity. The Security Rule requires covered entities to implement appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of ePHI.

INTRODUCTION

The **[Insert Group Health Plan Name]** (Health Plan) is a group health plan sponsored by **[Insert Company Name]** (Plan Sponsor). The Health Plan provides benefits solely through an insurance contract with a health insurance issuer or health maintenance organization (Issuer).

This Security Policy includes the Health Plan's policies and procedures for complying with applicable requirements of the HIPAA Security Rule when it (or the Plan Sponsor) creates or receives ePHI. The Plan Sponsor reserves the right to amend or change this Security Policy at any time (including retroactively).

This Security Policy does not create any third-party rights (including, but not limited to, rights of Health Plan participants, covered dependents and business associates). This policy is a guideline for compliance with the HIPAA Security Rule, and will not be binding on the Plan Sponsor to the extent it establishes requirements and obligations beyond those required by the HIPAA Security Rule. This policy does not address requirements under other federal laws or state laws. To the extent this policy conflicts with the applicable requirements of the HIPAA Security Rule, the Security Rule shall govern.

ACCESS TO PHI

Neither the Health Plan nor the Plan Sponsor create, receive, use or maintain ePHI on behalf of the Health Plan, with the exception of the following exempt information:

- Summary health information (as defined under 45 CFR § 164.504(a));
- Information on whether an individual is participating in the Health Plan, or is enrolled in or has disenrolled from an Issuer; or
- PHI that is provided to the Health Plan or Plan Sponsor pursuant to and in compliance with a valid HIPAA authorization under 45 CFR § 164.508.

The Health Plan and Plan Sponsor intend to comply with the HIPAA Security Rule, to the extent necessary to:

- Ensure the confidentiality, integrity and availability of all ePHI that the Health Plan creates, receives, maintains or transmits;
- Identify and protect against any reasonably anticipated threats or hazards to the security or integrity of this information;
- Protect against reasonably anticipated use or disclosure of this information that is not permitted or required under the HIPAA Privacy Rule; and
- Ensure its workforce complies with the procedures implemented to comply with the HIPAA Security Rule.

Except for functions that involve the exempt information described above, all of the Health Plan's functions, including functions involving ePHI, are handled by the Issuer.

DEFINITIONS

Except as otherwise described in this policy, all terms used shall have the definition given to them by the HIPAA Privacy and Security Rules, as applicable.

- *Business associate* – A person or organization that performs certain functions on behalf of, or provides certain services to, a covered entity that involves access to PHI.
- *Electronic protected health information (ePHI)* – Protected health information that is transmitted or maintained in electronic media.
- *Protected health information (PHI)* – Individually identifiable health information that is maintained or transmitted by a covered entity in any form (electronic, written or oral), subject to certain exclusions.
- *Summary health information* – Information, which may be individually identifiable, that summarizes the claims history, claims expenses or type of claims experienced by individuals for whom the plan sponsor has provided health benefits under a group health plan, and that is stripped of all individual identifiers other than five digit ZIP code.

COMPLIANCE REQUIREMENTS

Risk Assessment

Except for functions that involve the exempt information described above, all of the Health Plan's functions, including functions involving ePHI, are handled by the Issuer. The Issuer, as a separate covered entity, owns and controls the equipment, processes and policies for creating, receiving, using or maintaining ePHI relating to the Health Plan. The Issuer also has control of its employees, agents and subcontractors that have access to ePHI related to the Health Plan.

Because the Health Plan and the Plan Sponsor do not have access to or control over of the Issuer's security measures for ePHI, the Health Plan cannot evaluate or assess the potential risks or vulnerabilities to ePHI related to the Health Plan.

Security Standards

In deciding how to implement security measures, the Health Plan considered:

- Its size, complexity and capabilities;
- Its technical infrastructure, hardware and software security capabilities;
- The costs of security measures; and
- The probability and criticality of potential risks to health information.

Based on these factors and the risk assessment, the Health Plan has determined that it does not need to implement any of its own security standards to protect the confidentiality, integrity and availability of ePHI. The Issuer's security standards and specifications that relate to ePHI for the Health Plan are incorporated into the Health Plan's security policy, to the extent those standards and specifications are HIPAA compliant.

Accordingly, the Health Plan's security measures do not address the following standards and related implementation specifications:

- Security management process;
- Workforce security;
- Information access management;
- Security awareness management;
- Workstation use and security;
- Device and medial controls;
- Access control;
- Audit controls;

- Security incident procedures;
- Contingency plan;
- Evaluation;
- Facilities access controls;
- Integrity;
- Person or entity authentication; and
- Transmission security.

As part of their security management process, the Health Plan and the Plan Sponsor will periodically review their risk assessment and make any appropriate changes to these security standards in response to environmental or operational changes impacting the security of the Health Plan's ePHI, or any changes to the HIPAA Security Rules.

HIPAA policies and procedures that are controlled by the Health Plan shall be maintained for at least six years from the date of creation or date last in effect, whichever is later.

Security Official

[Insert name of employee or job title, for example, HR director] is the Security Official for the Health Plan. The Security Official is responsible for developing and implementing the Health Plan's security policies and procedures, including this policy.

Business Associates

If the Health Plan uses a business associate, it will receive satisfactory assurances from the business associate—through a business associate agreement—that the business associate will appropriately handle and safeguard PHI in compliance with HIPAA. If the Security Official knows about a pattern of activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation under the contract, the Security Official must take reasonable steps to cure the breach or end the violation, as applicable. If these steps were unsuccessful, the Security Official must analyze whether termination of the agreement is feasible.

SAMPLE HIPAA Breach Notification Policy

The HIPAA Breach Notification Rule (45 CFR §§ 164.400-414) requires HIPAA covered entities to notify affected individuals following the discovery of a breach of unsecured protected health information (PHI). Notification must also be provided to HHS and, in some cases, to the media.

INTRODUCTION

The **[Insert Group Health Plan Name]** (Health Plan) is a group health plan sponsored by **[Insert Company Name]** (Plan Sponsor). The Health Plan provides benefits solely through an insurance contract with a health insurance issuer or health maintenance organization (Issuer). Neither the Health Plan nor the Plan Sponsor create, receive, use or maintain ePHI on behalf of the Health Plan, with the exception of the following exempt information:

- Summary health information (as defined under 45 CFR § 164.504(a));
- Information on whether an individual is participating in the Health Plan, or is enrolled in or has disenrolled from an Issuer; or
- PHI that is provided to the Health Plan or Plan Sponsor pursuant to and in compliance with a valid HIPAA authorization under 45 CFR § 164.508.

To the extent that the Health Plan accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHI, the Health Plan will comply with the HIPAA Breach Notification Rule and provide the required notification to affected individuals, HHS and the media (when required) if the Health Plan or one of its business associates discovers a breach of unsecured PHI.

This policy includes the Health Plan's policies and procedures for complying with applicable requirements of the HIPAA Breach Notification Rule. The Plan Sponsor reserves the right to amend or change this policy at any time (including retroactively) without notice.

This policy does not create any third-party rights (including, but not limited to, rights of Health Plan participants, covered dependents and business associates). This policy is a guideline for compliance with the HIPAA Breach Notification Rule, and will not be binding on the Plan Sponsor to the extent it establishes requirements and obligations beyond those required by the HIPAA Breach Notification Rule. This policy does not address requirements under other federal laws or state laws. To the extent this policy conflicts with the applicable requirements of the HIPAA Breach Notification Rule, the Breach Notification Rule shall govern.

DEFINITIONS

Except as otherwise described in this policy, all terms used shall have the definition given to them by the HIPAA Privacy, Security and Breach Notification Rules, as applicable.

Breach – The acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI. A breach does not include:

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if the 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 the HIPAA Privacy Rule;
- Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, and the

information received is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or

- A disclosure of PHI 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.

An impermissible use or disclosure that does not fall under one of the three exceptions listed above is presumed to be a breach unless the covered entity or business associate demonstrates through a risk assessment that there is a low probability that the PHI has been compromised. This risk assessment must be based on at least the following four factors:

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

Additional factors may also need to be considered based on the circumstances of the impermissible use or disclosure.

Unsecured PHI – PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS. HHS designated encryption and destruction as the technologies and methodologies for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals.

COMPLIANCE REQUIREMENTS

The Plan Sponsor, on behalf of the Health Plan, shall investigate any incident that may constitute a breach of unsecured PHI and determine whether an impermissible use or disclosure has occurred. The Plan Sponsor will presume that an impermissible use or disclosure is a breach unless the Plan Sponsor's risk assessment demonstrates that there is a low probability that the PHI has been compromised. If the risk assessment does not show a low probability, the Plan Sponsor shall comply with the notification requirements as described below.

To Individuals

Following the discovery of a breach of unsecured PHI, the Plan Sponsor, on behalf of the Health Plan, shall notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of the breach. This notification must be made without unreasonable delay and I no case later than 60 calendar days of discovery of the breach.

To the Media

Following the discovery of a breach of unsecured PHI involving more than 500 residents of a state or jurisdiction, the Plan Sponsor, on behalf of the Health Plan, shall notify prominent media outlets serving the state or jurisdiction, in the form of a press release, at the same time notice is made to the individuals.

To HHS

Following a discovery of a breach of unsecured PHI, the Plan Sponsor, on behalf of the Health Plan, shall notify HHS as follows:

1. For breaches of unsecured PHI involving 500 or more individuals, this notification will be provided to HHS at the same time notice is made to the individuals.

2. For breaches of unsecured PHI involving fewer than 500 individuals, the Plan Sponsor shall maintain a log or other documentation of such breaches and, no later than 60 days after the end of each calendar year, provide the notification as instructed by HHS for breaches occurring during the previous calendar year.

BREACHES OF UNSECURED PHI HELD BY BUSINESS ASSOCIATES

Any business associate of the Health Plan that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHI shall be required to notify the Health Plan of a breach of unsecured PHI without unreasonable delay and no later than 60 calendar days after discovery of the breach. The notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired or disclosed during the breach. The business associate shall provide the Health Plan with any other information that the Health Plan is required to include in notification to the individual at the time of the notification (or promptly thereafter as information becomes available).

Upon receiving notification of a breach from a business associate, the Health Plan shall be responsible for notifying affected individuals, unless the Covered Entity and business associate otherwise agree that the business associate will provide such notice.

SAMPLE HIPAA POLICIES

FULLY INSURED HEALTH PLANS WITH ACCESS TO PHI

SELF-INSURED HEALTH PLANS

IMPORTANT – CUSTOMIZATION REQUIRED

The following are sample HIPAA policies for **fully insured health plans that are "hands-on" PHI** and **self-insured health plans**. These samples cannot be used "as is"—they **must be customized** for specific plan and employer information. Also, if the sample policies do not accurately reflect an employer's implementation of the HIPAA Rules, they should be customized for the employer's specific approach.

Because these policies assume that the health plan sponsor has access to PHI for plan administration functions, they incorporate a wide range of HIPAA compliance requirements. If a separate entity (for example, a third-party administrator or issuer) performs almost all of a health plan's administrative functions and the employer's access to PHI (and ePHI) is very limited, these policies can be revised to reflect that limited access. We encourage all customization to take place in coordination with knowledgeable benefits counsel.

Fully insured health plans that are **"hands-off" PHI** should not use these sample HIPAA policies. These health plans have fewer responsibilities under the HIPAA Rules.

Nothing in this toolkit should be considered as legal advice, including these sample documents. These sample documents are provided for educational and illustrative purposes only.

SAMPLE HIPAA Privacy Policy

The HIPAA Privacy Rule (45 CFR Part 160 and Part 164, subparts A and E) requires covered entities to comply with national standards for the privacy of protected health information (PHI). The Privacy Rule limits when an individual's PHI can be used or disclosed, gives individuals rights over their PHI and requires appropriate safeguards to protect the privacy of PHI.

INTRODUCTION

The **[Insert Group Health Plan Name]** (Health Plan) is a group health plan sponsored by **[Insert Company Name]** (Plan Sponsor). Members of the Plan Sponsor's workforce have access to PHI on behalf of the Plan itself or on behalf of the Plan Sponsor, to perform administrative functions for the Health Plan. The Health Plan and Plan Sponsor intend to comply with the HIPAA Privacy Rule, to the extent its requirements are applicable to the Health Plan.

This Privacy Policy includes the Health Plan's policies and procedures for complying with applicable requirements of the HIPAA Privacy Rule when it (or the Plan Sponsor) creates or receives PHI. The Plan Sponsor reserves the right to amend or change this Privacy Policy at any time (including retroactively) without notice, except to the extent notice is required under the HIPAA Privacy Rule.

This Privacy Policy does not create any third-party rights (including, but not limited to, rights of Health Plan participants, covered dependents and business associates). This policy is a guideline for compliance with the HIPAA Privacy Rule, and will not be binding on the Plan Sponsor to the extent it establishes requirements and obligations beyond those required by the HIPAA Privacy Rule. This policy does not address requirements under other federal laws or state laws. To the extent this policy conflicts with the applicable requirements of the HIPAA Privacy Rule, the Privacy Rule shall govern.

DEFINITIONS

Except as otherwise described in this policy, all terms used shall have the definition given to them by the HIPAA Privacy and Security Rules, as applicable.

- *Business associate* – A business associate is an entity that: (1) creates, receives, maintains or transmits PHI on behalf of a covered entity (including for claims processing or administration, data analysis or underwriting); or (2) provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation or financial services to a covered entity, where the performance of those services involves access to PHI.
- *Covered entity* – A health plan, health care clearinghouse or health care provider who transmits any health information in electronic form in connection with a HIPAA-covered transaction.
- *Designated record set* – A group of records maintained by or for the Health Plan that is:
    - The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for the Plan; or
    - Used, in whole or in part, by or for the Health Plan to make decisions about individuals.
- *Plan administration functions* – Administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan, including payment and health care operation activities. This excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.
- *Protected health information (PHI)* – Information that is created or received by (or on behalf of) the Health Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision

of health care to a participant; or the past, present or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. For purposes of this Privacy Policy, PHI does not include:

  - Summary health information that is disclosed to the Plan Sponsor for the purpose of obtaining premium bids, or modifying, amending or terminating the Health Plan;
  - Enrollment and disenrollment information for the Health Plan;
  - PHI that is disclosed to the Health Plan or the Plan Sponsor pursuant to a valid HIPAA authorization; and
  - Employment records that are created or received by the Plan Sponsor in its role as an employer, and not as a sponsor of the Health Plan.

- *Summary health information* – Information, which may be individually identifiable, that summarizes the claims history, claims expenses or type of claims experienced by individuals for whom the plan sponsor has provided health benefits under a group health plan, and that is stripped of all individual identifiers other than five digit ZIP code.

GENERAL REQUIREMENTS

Designation of Privacy Officer and Contact Person

[Insert position title (e.g., Director of Human Resources) or individual's name] is the Privacy Officer for the Health Plan. The Privacy Officer is responsible for the development and implementation of the Health Plan's policies and procedures relating to the privacy of PHI. The Privacy Officer will work with the Health Plan's Security Official with respect to electronic PHI (ePHI).

The Privacy Officer is responsible for ensuring that the Health Plan complies with all applicable requirements of the HIPAA Privacy Rule, including the use and disclosure rules and individual rights requirements. The Privacy Officer will also make sure there is a valid business associate agreement in place with each business associate for the Health Plan, and will monitor each business associate's compliance with the terms of its agreement.

[Insert position title (e.g., Director of Human Resources) or individual's name] is the contact person for receiving complaints regarding the privacy of PHI and answering questions about the Health Plan's privacy practices.

Workforce Training

The Plan Sponsor will train all members of its workforce who have access to PHI on the Health Plan's policies and procedures with respect to PHI. The Privacy Officer is responsible for developing and implementing this training program to provide the necessary and appropriate training in order for workforce members to carry out their functions in compliance with HIPAA.

> ***Compliance Step for Employer*** – Implement a HIPAA training program for employees who have access to PHI

Each workforce member who has access to PHI will receive HIPAA training within a reasonable period of time after they join the workforce. Training will also be provided for all affected workforce members when there is a material change in the Health Plan's HIPAA policies and procedures.

***Privacy Notice** [select option that applies to the plan and delete the other option]*

[Option 1 - Fully insured health plans]

Individuals who enroll in the Health Plan will receive a Notice of Privacy Practices (Privacy Notice) from the health insurance issuer or health maintenance organization (Issuer) with respect to the Health Plan. The Privacy Notice explains the Issuer's privacy practices, including how PHI is used and disclosed by the Issuer, individuals' rights under the HIPAA Privacy Rule, and the Issuer's legal responsibilities under HIPAA with respect to PHI.

The Privacy Notice will be provided by the Issuer to Health Plan enrollees at the time of their initial enrollment and upon request. Not less frequently that once every three years, the Issuer will notify covered individuals about the availability of the Privacy Notice and how to obtain a copy of it. The Issuer must provide an updated Privacy Notice if there is a material change to the Notice.

The Privacy Official is responsible for developing and maintaining the Health Plan's own Privacy Notice. The Health Plan's Privacy Notice will describe the Plan Sponsor's access to PHI for plan administrative functions and the Plan's compliance with the HIPAA Privacy Rule, including:

- The uses and disclosures of PHI that may be made by the Health Plan;
- Individuals' rights under the Privacy Rule; and
- The Health Plan's legal duties with respect to the PHI.

The Health Plan must provide this notice to any person upon request.

Compliance Step for Employer – Create and maintain a Privacy Notice. See this toolkit's sample Privacy Notice.

[Option 2 – Self-insured health plans]

The Privacy Official is responsible for developing and maintaining a Notice of Privacy Practices (Privacy Notice) for the Health Plan. The Privacy Notice will describe the Plan Sponsor's access to PHI for plan administrative functions and the Plan's compliance with the HIPAA Privacy Rule, including:

- The uses and disclosures of PHI that may be made by the Health Plan;
- Individuals' rights under the Privacy Rule;
- The Health Plan's legal duties with respect to the PHI; and
- Other information required by the Privacy Rule.

The Privacy Notice will be provided to Health Plan participants at the time of their initial enrollment and upon request. Not less frequently than once every three years, the Health Plan will notify covered individuals about the availability of the Privacy Notice and how to obtain a copy of it. The Health Plan will provide an updated Privacy Notice if there is a material change to the Notice. If the Plan Sponsor maintains a website that provides information about the Health Plan, the Privacy Notice will be posted on the website.

Compliance Step for Employer – Create and provide a Privacy Notice. See this toolkit's sample Privacy Notice.

Complaints

The contact person accepts complaints about the Health Plan's privacy practices. The Privacy Official is responsible for creating a process for individuals to make complaints about the Health Plan's privacy practices and a system for handling individuals' complaints.

Compliance Step for Employer – Create a process for complaints

Sanctions

The HIPAA Privacy Rule requires the Health Plan to have and apply appropriate sanctions against workforce members who fail to comply with these privacy practices or who otherwise violate the Privacy Rule. Accordingly, workforce members who use or disclose PHI in violation of HIPAA or this Privacy Policy will be subject to **[Insert reference to an established Company discipline policy or describe disciplinary procedures that apply to HIPAA violations]**.

Mitigation

The Health Plan will mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of PHI that is in violation of this Privacy Policy or HIPAA. Any workforce member or business associate who knows of an impermissible use or disclosure of PHI must immediately contact the Privacy Official so that the Privacy Official may take steps to mitigate any harmful effect of the impermissible use or disclosure.

No Intimidation or Retaliatory Acts

The Health Plan (and the Plan Sponsor) will not threaten, intimidate, coerce, harass, discriminate against or take any other retaliatory action against any individual for:

- Exercising their rights under the HIPAA Privacy Rule;
- Participating in any process provided under the HIPAA Privacy Rule, including the filing of a complaint;
- Testifying, assisting or participating in an investigation, compliance review, proceeding or hearing under HIPAA; or
- Opposing any act or practice that is unlawful under HIPAA, provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Rule.

No Waiver of Rights

The Health Plan may not require individuals to waive their privacy rights under HIPAA as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

Plan Document Amendment

In order for the Health Plan to disclose PHI to the Plan Sponsor (or to provide for or permit the disclosure of PHI to the Plan Sponsor), the Plan's documents must be amended to establish the permitted and required uses and disclosures of PHI by the Plan Sponsor and require the Plan Sponsor to:

- Not use or further disclose PHI other than as permitted by the Plan's documents or required by law;
- Ensure that any agents or subcontractors to whom it provides PHI received from the Health Plan agree to the same restrictions and conditions that apply to the Plan Sponsor;
- Not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor;
- Report to the Privacy Official any use or disclosure of PHI that is inconsistent with the permitted uses and disclosures;

- Make PHI available to Health Plan participants in accordance with the Privacy Rule's requirements for access, amendment and accounting, to the extent applicable;
- Make its internal practices, books and records relating to the use and disclosure of PHI received from the Health Plan available to the Department of Health and Human Services (HHS) upon request;
- If feasible, return or destroy all PHI received from the Health Plan that the Plan Sponsor still maintains in any form and retain no copies of the information when no longer needed for the purposes for which disclosure was made, except that, if the return or destruction is not feasible, limit further uses and disclosures to those that make the return or destruction of the information infeasible; and
- Ensure adequate separation between the Health Plan and the Plan Sponsor, as required by the HIPAA Privacy Rule.

Compliance Step for Employer – Adopt a plan amendment. See this toolkit's sample plan amendment.

Safeguards for PHI

The Plan Sponsor, on behalf of the Health Plan, will establish appropriate administrative, technical and physical safeguards to protect the privacy of PHI. These safeguards, which will be documented by the Privacy Official, will be designed to protect PHI from any intentional or unintentional use or disclosure that would violate the HIPAA Privacy Rule. The Privacy Official will also establish rules to ensure adequate separation between workforce members who have access to PHI for plan administration functions and other workforce members who do not have access to PHI.

Compliance Step for Employer – Establish and document these administrative, technical and physical safeguards.

Documentation

The Health Plan's Privacy Policy and related procedures will be documented and maintained for at least six years from the date they were last in effect. This Privacy Policy and related procedures will be updated, as necessary, to comply with changes in the law or any changes in the Health Plan's operations or environment.

The Health Plan will also maintain documentation of any communication required under the Privacy Rule, and any actions, activities or designations that must be documented under HIPAA, such as HIPAA authorizations, the Privacy Notice, individuals' privacy rights requests and sanctions for violations of the Health Plan's privacy practices. This documentation will also be maintained for at least six years.

Personal Representatives

The Health Plan treats an individual's personal representative as the individual with respect to uses and disclosures of the individual's PHI, as well as the individual's rights under the Privacy Rule.

USE AND DISCLOSURE OF PHI

General Rules

The Health Plan may use and disclose PHI only as required or permitted under the HIPAA Privacy Rule and this Privacy Policy. All workforce members must comply with the Health Plan's use and disclosure rules for PHI.

A workforce member cannot use PHI for the purposes of another benefit or employee benefit plan (for example, a disability or life insurance plan), unless an individual has authorized the use through a valid HIPAA authorization. Also, the Plan Sponsor cannot use PHI obtained from the Health Plan in connection with employment-related actions and decisions.

Permitted Disclosures for Treatment, Payment and Health Care Operations

The Health Plan may use and disclose PHI:

- For the Plan's own payment and health care operations;
- To another covered entity or a health care provider for the payment activities of the receiving entity;
- For the treatment activities of a health care provider; and
- To another covered entity for purposes of the other covered entity's health care operations if the other covered entity has (or had) a relationship with the participant and the PHI pertains to that relationship, subject to the approval of the Privacy Officer.

All of these permitted uses and disclosures of PHI are subject to the minimum necessary standard.

Treatment means the provision, coordination or management of health care and related services by one or more health care providers.

Payment means activities undertaken by the Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Plan, or to provide reimbursement for the provision of health care. Payment also includes:

- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost-sharing amounts and the adjudication or subrogation of health benefit claims);
- Risk adjusting based on enrollee health status and demographic characteristics;
- 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;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care or justification of charges; and
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

Health care operations means any of the following activities of the Health Plan to the extent that the activities are related to plan administration:

- Conducting quality assessment and improvement activities;
- Reviewing health plan performance;
- Underwriting, enrollment, premium rating and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits;
- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;
- Business planning and development; and

- Business management and general administrative activities of the Health Plan.

Required Disclosures of PHI

The Health Plan must disclose PHI, in accordance with the HIPAA Privacy Rule, in the following situations:

- An individual (or the individual's personal representative) requests a disclosure of their own PHI; or
- The disclosure is requested by HHS in order to investigate the Health Plan's compliance with HIPAA.

The Privacy Official must review and approve these requests for PHI before any PHI is disclosed.

Other Permissible Uses and Disclosures

The Health Plan is permitted to use or disclose PHI in the following situations, without an individual's authorization, when specific requirements contained in the HIPAA Privacy Rule (45 CFR § 164.512) are satisfied, subject to the Privacy Official's approval:

- Uses and disclosures that are required by law;
- Uses and disclosures for public health activities;
- Disclosures about victims of abuse, neglect or domestic violence;
- Uses and disclosures for health oversight activities;
- Disclosures for judicial and administrative proceedings;
- Disclosures for law enforcement purposes;
- Uses and disclosures about decedents;
- Uses and disclosures for cadaveric organ, eye or tissue donation purposes;
- Uses and disclosures for certain limited research purposes;
- Uses and disclosures to avert a serious threat to health or safety;
- Uses and disclosures for specialized government functions; and
- Disclosures for workers' compensation programs.

The Health Plan must comply with the minimum necessary standard, as applicable, when using or disclosing PHI for these purposes.

Special Rules for PHI Related to Reproductive Health Care

Effective Dec. 23, 2024, the Health Plan must comply with restrictions on the use and disclosure of PHI related to reproductive health care, as set forth in a final rule issued by HHS on April 26, 2024. To comply with the final rule, the Health Plan is prohibited from using or disclosing PHI for the criminal, civil or administrative investigation of (or proceeding against) any person in connection with seeking, obtaining, providing or facilitating reproductive health care where such health care is lawful under the circumstances in which it is provided. The Health Plan is also prohibited from identifying any person for the purpose of initiating such an investigation or proceeding.

In addition, the Health Plan must obtain a valid attestation when a request is made to use or disclose PHI potentially related to reproductive health care for purposes of health oversight activities, judicial and administrative proceedings, law enforcement purposes, or disclosures to coroners or medical examiners to ensure that the use or disclosure is not for a prohibited purpose.

Before PHI potentially related to reproductive health care is used or disclosed, the Privacy Official must verify that the use or disclosure is permissible under the final rule, including confirming that an attestation is valid under HIPAA, if applicable.

De-identified Information

The Health Plan may freely use and disclose PHI that has been de-identified in accordance with the HIPAA Privacy Rule. 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 methods for de-identifying PHI—a professional statistical method and a method that removes 18 specific identifiers. Before using or disclosing de-identified PHI, workforce members must receive the Privacy Official's verification that the PHI has been appropriately de-identified.

Authorized Disclosures

PHI may be disclosed for any purpose if an authorization that satisfies all of the HIPAA Privacy Rule's requirements for a valid authorization is provided by the individual who is the subject of the PHI (or their personal representative). Any use or disclosure of PHI made pursuant to a signed HIPAA authorization must be consistent with the terms and conditions of the authorization. Before PHI is disclosed pursuant to an authorization, the Privacy Official must verify the individual's identity and confirm that the authorization form is valid under HIPAA.

Disclosures to Plan Sponsor

The Health Plan may disclose PHI to the Plan Sponsor for plan administration functions. Only the following workforce members will have access to PHI for plan administration functions: **[Insert description of employees by title, department or name]**. Workforce members with access to PHI will receive training on the Health Plan's privacy practices, and must comply with this Privacy Policy and any additional privacy procedures implemented by the Privacy Official.

Workforce members with access to PHI may not disclose PHI to other workforce members, unless the disclosure is made pursuant to an individual's valid HIPAA authorization or the disclosure has been approved by the Privacy Official as being compliant with HIPAA and this Privacy Policy. Workforce members with access to PHI must take all appropriate steps to ensure that PHI is not used or disclosed for employment purposes or in connection with another benefit or benefit plan maintained by the Plan Sponsor.

PHI that is disclosed to the Plan Sponsor may not be used for employment-related actions and decisions. It also may not be used in connection with any other benefit or employee benefit plan of the Plan Sponsor, unless authorized by the individual pursuant to a valid HIPAA authorization.

Minimum Necessary Standard

When using or disclosing PHI (or when requesting PHI from another covered entity or business associate), the Health Plan will make a reasonable effort to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. This minimum necessary standard does not apply to any of the following:

- Uses and disclosures made to the individual who is the subject of PHI;
- Uses or disclosures made pursuant to a valid HIPAA authorization;
- Disclosures made to HHS;
- Uses or disclosures that are required by law; and
- Uses and disclosures that are required to comply with HIPAA.

For any disclosure that the Health Plan makes on a routine and recurring basis, the Privacy Official will implement protocols for limiting the disclosure of PHI to the amount reasonably necessary to achieve the purpose of the disclosure. All other disclosures must be reviewed with the Privacy Official on an individual basis to ensure that the disclosure complies with the minimum necessary standard.

When requesting PHI from another covered entity, the Health Plan must limit its request to the PHI that is reasonably necessary to accomplish the purpose for which the request is made. For routine and recurring requests, the Privacy Official will implement protocols for limiting the request for PHI to the amount reasonably necessary to achieve the purpose of the request. All other requests must be reviewed with the Privacy Official on an individual basis to ensure that the request complies with the minimum necessary standard.

Disclosures to Business Associates

The Health Plan may disclose PHI to a business associate, and may allow a business associate to create, receive, maintain or transmit PHI on its behalf if the Health Plan obtains satisfactory assurances from the business associate that it will appropriately safeguard the information. This assurance must be in the form of a HIPAA-compliant business associate agreement.

The Privacy Official will maintain a list of all business associates for the Health Plan and their corresponding business associate agreements. Before sharing information with a business associate, a workforce member must contact the Privacy Official to verify that a business associate agreement is in effect.

> ***Compliance Step for Employer*** – The Privacy Officer should identify all business associates and confirm that business associate agreements are in place.

INDIVIDUAL RIGHTS

The Health Plan will provide individuals with specific rights to their PHI as required under the HIPAA Privacy Rule and explained in this Privacy Policy.

Right to Access PHI

An individual has the right to inspect and obtain a copy of their PHI held in a designated record set by the Health Plan or a business associate, for as long as the PHI is maintained in the designated record set. The Health Plan will provide individuals with access to their PHI in compliance with the HIPAA Privacy Rule (45 CFR § 164.524).

Individuals must send their requests for access in writing to the Health Plan's contact person, who will review the request with the Privacy Official. The Privacy Official must verify the individual's identity and analyze whether the requested PHI is held in a designated record set. Requests for access cannot be approved or denied without approval from the Privacy Official.

The Health Plan will provide individuals with access to their PHI as soon as possible, but no later than 30 days after the receipt of a request that is approved. This 30-day period may be extended by another 30 days if the Health Plan explains the reasons for the delay and the estimated response date before the end of the initial 30-day period.

In general, the Health Plan will not deny an individual's valid request for access to their PHI held in a designated record set. However, if the request is denied based on an exception to the right of access, the Privacy Official will provide the individual with a written denial, in accordance with the Privacy Rule's requirements.

The Health Plan will provide an individual with access to the PHI in the form and format requested by the individual, if it is readily producible in that form and format or, if it is not, in a readable hard copy form or other form as agreed to by

the Health Plan and the individual. However, if the requested PHI is maintained electronically and the individual requests an electronic copy of the information, the Health Plan must provide the individual with access to the PHI in the electronic form and format requested if it is readily producible in that form and format or, if it is not, in a readable electronic form and format as agreed to by the Health Plan and the individual.

The Health Plan may impose a reasonable, cost-based fee for copies of requested PHI, provided that the fee may only include the cost of:

- Labor for copying the PHI requested by the individual;
- Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; and
- Postage, when an individual has requested that the copy be mailed.

Right to Amend PHI

An individual has the right to request an amendment or correction to their PHI held in a designated record set by the Health Plan or a business associate, for as long as the PHI is maintained in the designated record set. The Health Plan will comply with an individual's right to an amendment of their PHI in accordance with the HIPAA Privacy Rule (45 CFR § 164.526).

Individuals must send their requests for amendment in writing to the Health Plan's contact person and identify the reason that supports the request. The contact person will review the request with the Privacy Official. Requests for an amendment cannot be approved or denied without approval from the Privacy Official.

The Health Plan will act on an individual's request for an amendment no later than 60 days after receiving the request. If the Health Plan is unable to act on the amendment within this time period, it may extend the time period by no more than 30 days if the Health Plan explains the reasons for the delay and the estimated response date before the end of the initial 60-day period.

The Health Plan may deny an individual's request for an amendment if the PHI:

- Was not created by the Health Plan (unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment);
- Is not part of the designated record set;
- Is not subject to the right of access described above; or
- Is accurate and complete.

If an individual's request for an amendment of their PHI is denied, the Privacy Official will provide the participant with a written explanation of the reasons for the denial, the individual's right to submit a statement disagreeing with the denial and the Health Plan's complaint procedure.

Right to an Accounting of PHI

The Health Plan will provide individuals with an accounting of disclosures of their PHI as required by the HIPAA Privacy Rule (45 CFR § 164.528). An individual has the right to an accounting of disclosures of PHI made by the Health Plan in the six years prior to the date of the request, except for disclosures:

- To carry out treatment, payment or health care operations;
- To individuals about their own PHI;
- Incident to an otherwise permitted or required use or disclosure;

- Pursuant to a HIPAA authorization;
- To people involved in the individual's care or other notification purposes;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials; or
- As part of a limited data set.

Individuals must send their requests for an accounting to the Health Plan's contact person. The contact person will review the request with the Privacy Official. Requests for an accounting cannot be approved or denied without approval from the Privacy Official.

The Health Plan will act on an individual's request for an accounting no later than 60 days after receiving the request. If the Health Plan is unable to act on the amendment within this time period, it may extend the time period by no more than 30 days if the Health Plan explains the reasons for the delay and the estimated response date before the end of the initial 60-day period.

The accounting must include the date of the disclosure, the name of the entity or person who received the PHI, a brief description of the PHI disclosed and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The Health Plan will provide the first accounting in any 12-month period free of charge. The Health Plan may impose a reasonable fee for providing additional accountings.

Requests for Confidential Communications

The Health Plan permits individuals to request to receive communications of PHI from the Plan by alternative means or at an alternative location. The Health Plan will accommodate reasonable requests for confidential communications in accordance with the HIPAA Privacy Rule (45 CFR § 164.522) when an individual states that the disclosure of all or part of the information could endanger the individual.

Individuals must send their requests for confidential communications in writing to the Health Plan's contact person. The contact person will review the request with the Privacy Official. Requests for confidential communications cannot be approved or denied without approval from the Privacy Official.

Requests for Restrictions on Use and Disclosure of PHI

The Health Plan permits individuals to request restrictions on the use and disclosure of their PHI. Individuals must send their requests for confidential communications in writing to the Health Plan's contact person. The contact person will review the request with the Privacy Official.

The Health Plan, may (but is not required to) agree to the requested restrictions, as provided in the HIPAA Privacy Rule (45 CFR § 164.522). Requests for restrictions cannot be approved or denied without approval from the Privacy Official.

SAMPLE HIPAA Security Policy

The HIPAA Security Rule (45 CFR Part 160 and Part 164, subparts A and C) establishes national standards to protect individuals' electronic protected health information (ePHI) that is created, received, used or maintained by a covered entity. The Security Rule requires covered entities to implement appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of ePHI.

INTRODUCTION

The **[Insert Group Health Plan Name]** (Health Plan) is a group health plan sponsored by **[Insert Company Name]** (Plan Sponsor). Members of the Plan Sponsor's workforce have access to PHI on behalf of the Plan itself or on behalf of the Plan Sponsor, to perform administrative functions for the Health Plan. The Health Plan and Plan Sponsor intend to comply with the HIPAA Security Rule, to the extent necessary to:

- Ensure the confidentiality, integrity and availability of all ePHI that the Health Plan creates, receives, maintains or transmits;
- Identify and protect against any reasonably anticipated threats or hazards to the security or integrity of this information;
- Protect against reasonably anticipated use or disclosure of this information that is not permitted or required under the HIPAA Privacy Rule; and
- Ensure its workforce complies with the procedures implemented to comply with the HIPAA Security Rule.

This Security Policy includes the Health Plan's policies and procedures for complying with applicable requirements of the HIPAA Security Rule when it (or the Plan Sponsor) creates or receives ePHI. The Plan Sponsor reserves the right to amend or change this Security Policy at any time (including retroactively).

This Security Policy does not create any third-party rights (including, but not limited to, rights of Health Plan participants, covered dependents and business associates). This policy is a guideline for compliance with the HIPAA Security Rule, and will not be binding on the Plan Sponsor to the extent it establishes requirements and obligations beyond those required by the HIPAA Security Rule. This policy does not address requirements under other federal laws or state laws. To the extent this policy conflicts with the applicable requirements of the HIPAA Security Rule, the Security Rule shall govern.

DEFINITIONS

Except as otherwise described in this policy, all terms used shall have the definition given to them by the HIPAA Privacy and Security Rules, as applicable.

- *Business associate* – A business associate is an entity that: (1) creates, receives, maintains or transmits PHI on behalf of a covered entity (including for claims processing or administration, data analysis or underwriting); or (2) provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation or financial services to a covered entity, where the performance of those services involves access to PHI.
- *Covered entity* – A health plan, health care clearinghouse or health care provider who transmits any health information in electronic form in connection with a HIPAA-covered transaction.
- *Electronic media* – Electronic storage material on which data is or may be recorded electronically (including devices on computers and any removable or transportable digital memory medium) or transmission media used to exchange information already in electronic storage media (including, the internet, leased lines, private networks and the physical movement of removable or transportable electronic storage media). Certain transmissions, including paper, facsimile and voice via telephone, are not considered to be transmissions via

electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

- *Electronic protected health information (ePHI)* – Protected health information that is transmitted or maintained in electronic media.
- *Plan administration functions* – Administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan, including payment and health care operation activities. This excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.
- *Protected health information (PHI)* – Information that is created or received by (or on behalf of) the Health Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. For purposes of this Privacy Policy, PHI does not include:
    - Summary health information that is disclosed to the Plan Sponsor for the purpose of obtaining premium bids, or modifying, amending or terminating the Health Plan;
    - Enrollment and disenrollment information for the Health Plan;
    - PHI that is disclosed to the Health Plan or the Plan Sponsor pursuant to a valid HIPAA authorization; and
    - Employment records that are created or received by the Plan Sponsor in its role as an employer, and not as a sponsor of the Health Plan.
- *Summary health information* – Information, which may be individually identifiable, that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom the plan sponsor has provided health benefits under a group health plan, and that is stripped of all individual identifiers other than five digit ZIP code.

RISK ASSESSMENT

DRAFTING TIPS

The Security Rule requires a covered entity to conduct an accurate and thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the covered entity. This is a crucial first step in a covered entity's efforts to comply with the Security Rule. It directs what reasonable steps the covered entity should take to protect the ePHI it creates, transmits, receives or maintains. Risk assessment is also an ongoing process. Covered entities should periodically revisit their risk assessments and make appropriate updates to their ePHI safeguards.

The Security Rule **requires the risk assessment to be documented** but does not require a specific format. There are numerous methods of performing risk analysis and there is no single method or best practice that guarantees compliance with the Security Rule. However, there are some common risk assessment steps, as described in this toolkit. In addition, HHS, through its Office of the National Coordinator for Health Information Technology, has developed an **interactive Security Risk Assessment Tool** (SRA Tool) to assist covered entities in performing and documenting security risk assessments. Although HHS designed the SRA Tool for health care providers in small to medium-sized offices, it is a helpful resource for all covered entities to review their implementation of the HIPAA Security Rule. This tool is available here.

[Insert documentation of the Health Plan's risk assessment and delete the drafting tips box above]

SECURITY SAFEGUARDS

In deciding how to implement security measures, the Health Plan considered:

- Its size, complexity and capabilities;
- Its technical infrastructure, hardware and software security capabilities;
- The costs of security measures; and
- The probability and criticality of potential risks to health information.

Based on these factors and the risk assessment, the Health Plan has implemented the following security safeguards:

DRAFTING TIPS

The security measures implemented by a health plan will largely depend on the Plan's access to ePHI. A self-funded health plan that is administered by the Plan Sponsor (that is, a self-administered plan) will need to implement a full range of security measures. A health plan that uses an issuer or third-party administrator for plan administration may have fewer security responsibilities, depending on whether the plan's ePHI is maintained on equipment and media owned and controlled by the issuer or TPA.

Also, in an effort to provide covered entities with additional flexibility, the Security Rule categorizes certain standards as "addressable." The addressable designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.

[Customize the following chart for the security standards implemented by the Health Plan, based on the Plan's risk assessment. Delete the drafting tips box above.]

ADMINISTRATIVE SAFEGUARDS	
Security Management Process	The Health Plan has implemented the following security measures to prevent, detect, contain and correct security violations: **[Insert description of security procedures, including the following:** • **Risk management** – Description of security measures to reduce risks and vulnerabilities to a reasonable and appropriate level; • **Sanction policy** – Description of disciplinary procedures that apply to HIPAA violations; and • **Information system activity review** – Description of procedures for the regular review of records related to information system activity, such as reviewing audit logs, access reports and security incident tracking reports.]

Assigned security responsibility	**[Insert name of employee or job title, for example, HR director]** is the Security Official for the Health Plan. The Security Official is responsible for developing and implementing the Health Plan's security policies and procedures, including this policy. The Security Official will coordinate the Health Plan's security activities with the Health Plan's Privacy Officer.
Workforce security	The Health Plan has implemented the following procedures to ensure that all members of its workforce have appropriate access to ePHI for plan administration functions and to prevent other workforce members who do not have authorized access to ePHI from obtaining access to this information: **[Insert description of workforce security procedures, including the following implementation specifications:** • **Authorization and/or supervision** *(addressable)* – Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed; • **Workforce clearance procedures** *(addressable)* – Implement procedures to determine that the access of a workforce member to ePHI is appropriate; and • **Termination procedures** *(addressable)* – Implement procedures for terminating access to ePHI when the employment of, or other arrangement with, a workforce member ends.]
Information access management	The Health Plan has implemented the following procedures for authorizing access to ePHI that are consistent with the HIPAA Privacy Rule's requirements: **[Insert description of the procedures for authorizing access to ePHI, including the following implementation specifications:** • **Access authorization** *(addressable)* – Implement procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process or other mechanism; • **Access establishment and modification** *(addressable)* – Implement procedures that, based on the Health Plan's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program or process.]
Security awareness and training	The Health Plan has implemented the following security awareness and training program for workforce members: **[Insert description of Plan's security awareness and training program, including the following implementation specifications:** • **Security reminders** *(addressable)* – Periodic security updates; • **Protection from malicious software** *(addressable)* – Procedures for guarding against, detecting and reporting malicious software; • **Login monitoring** *(addressable)* – Procedures for monitoring login attempts and reporting discrepancies;

	• **Password management** *(addressable)* – Procedures for creating, changing and safeguarding passwords.]
Security incident procedures	The Health Plan has implemented the following security incident procedures: **[Insert description of Plan's procedures for:** • **Identifying and responding to suspected or known security incidents;** • **Mitigating, to the extent practicable, harmful effects of known security incidents; and** • **Documenting security incidents and their outcomes.]**
Contingency plan	The Health Plan has implemented the following contingency plan: **[Insert description of Plan's procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain ePHI, including the following implementation specifications:** • **Data backup plan** – Procedures to create and maintain retrievable exact copies of ePHI; • **Disaster recovery plan** – Procedures to restore any loss of data; • **Emergency mode operation plan** – Procedures to enable continuation of critical business process for protection of the security of ePHI while operating in emergency mode; • **Testing and revision procedures** *(addressable)* – Procedures for periodic testing and revision of contingency plans; and • **Applications and data criticality analysis** *(addressable)* – Assess the relative criticality of specific applications and data in support of other contingency plan components.]
Evaluation	The Health Plan will perform a periodic technical and nontechnical evaluation, in response to environmental or operational changes affecting the security of ePHI, that establish the extent to which the Health Plan's security policies and procedures meet the requirements of the HIPAA Security Rule.
PHYSICAL SAFEGUARDS	
Facility access controls	The Health Plan has implemented the following facility access controls: **[Insert description of Plan's procedures to limit physical access to its electronic information systems and the facility in which they are housed, while ensuring that properly authorized access is allowed, including the following implementation specifications:** • **Contingency operations** *(addressable)* – Procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency;

	• **Facility security plan** *(addressable)* – Procedures to safeguard the facility and the equipment contained in the facility from unauthorized physical access, tampering and theft; • **Access control and validation** *(addressable)* – Procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision; and • **Maintenance records** *(addressable)* – Procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors and locks).]
Workstation use	The Health Plan has implemented the following security procedures regarding workstation use: **[Insert description of the proper functions to be performed, the manner in which those functions are to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.]**
Workstation security	The Health Plan has implemented the following physical safeguards for all workstations that access ePHI, to restrict access to authorized users: **[Insert description of physical safeguards]**.
Device and media controls	The Health Plan has implemented the following procedures that govern the receipt and removal of hardware and electronic media that contain ePHI: • **Disposal** – Description of the Plan's procedures for the final disposition of ePHI and/or the hardware or electronic media on which it is stored; • **Media reuse –** Description of Plan's procedures for removal of ePHI from electronic media before the media are made available for reuse; • **Accountability** *(addressable)* – The Plan will maintain a record of the movements of hardware and electronic media and any responsible person; and • **Data backup and storage** *(addressable)* – The Plan will create a retrievable, exact copy of ePHI, when needed, before movement of equipment.
TECHNICAL SAFEGUARDS	
Access controls	The Health Plan has implemented the following procedures for electronic information systems that maintain ePHI to allow access only to those people or software programs that have been granted access rights in accordance with the Health Plan's security procedures: • **Unique user identification** – Describe assignment of a unique name and/or number for identifying and tracking user identity; • **Emergency access** – Description of Plan's procedures for obtaining necessary ePHI during an emergency; • **Automatic logoff** *(addressable)* – Description of procedures for terminating an electronic session after a predetermined time of inactivity; and

	• **Encryption and decryption** *(addressable)* – Description of mechanism to encrypt and decrypt ePHI.
Audit controls	The Health Plan has implemented the following audit controls for ePHI: **[Insert description of Plan's hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI]**.
Integrity	The Health Plan has implemented the following procedures to protect ePHI from improper alteration or destruction: **[Insert description of safeguards, including the following:** • **Authentication mechanism** *(addressable)* – Describe mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.]
Person or entity authentication	The Health Plan has implemented the following procedures to verify that a person or entity seeking access to ePHI is the one claimed: **[Insert description of authentication procedures]**.
Transaction security	The Health Plan has implemented the following technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network**: [Insert description of transaction security procedures, including the following:** • **Integrity controls** *(addressable)* – Description of security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of; and • **Encryption** *(addressable)* – Description of mechanism to encrypt ePHI whenever deemed appropriate.]
ORGANIZATION REQUIREMENTS	
Business associates	If the Health Plan uses a business associate, it will receive satisfactory assurances from the business associate—through a business associate agreement—that the business associate will appropriately handle and safeguard PHI in compliance with HIPAA. If the Security Official knows about a pattern of activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation under the contract, the Security Official must take reasonable steps to cure the breach or end the violation, as applicable. If these steps were unsuccessful, the Security Official must analyze whether termination of the agreement is feasible.
Health Plan documents	In order for the Health Plan to disclose PHI to the Plan Sponsor (or to provide for or permit the disclosure of PHI to the Plan Sponsor), the Plan's documents must be amended to provide that the Plan Sponsor will reasonably and appropriate safeguard ePHI created, received, maintained, or transmitted to or by the Plan Sponsor on behalf of the Health Plan.

Security documentation	The Health Plan's Security Policy and related procedures will be documented and maintained for at least six years from the date they were last in effect. This Security Policy and related procedures will be updated, as necessary, to comply with changes in the law or any changes in the Health Plan's operations or environment.

SAMPLE HIPAA Breach Notification Policy

The HIPAA Breach Notification Rule (45 CFR §§ 164.400-414) requires HIPAA covered entities to notify affected individuals following the discovery of a breach of unsecured protected health information (PHI). Notification must also be provided to HHS and, in some cases, to the media.

INTRODUCTION

The **[Insert Group Health Plan Name]** (Health Plan) is a group health plan sponsored by **[Insert Company Name]** (Plan Sponsor). To the extent that the Health Plan accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHI, the Health Plan will comply with the HIPAA Breach Notification Rule and provide the required notification to affected individuals, HHS and the media (when required) if the Health Plan or one of its business associates discovers a breach of unsecured PHI.

This policy includes the Health Plan's policies and procedures for complying with applicable requirements of the HIPAA Breach Notification Rule. The Plan Sponsor reserves the right to amend or change this policy at any time (including retroactively) without notice.

This policy does not create any third-party rights (including, but not limited to, rights of Health Plan participants, covered dependents and business associates). This policy is a guideline for compliance with the HIPAA Breach Notification Rule, and will not be binding on the Plan Sponsor to the extent it establishes requirements and obligations beyond those required by the HIPAA Breach Notification Rule. This policy does not address requirements under other federal laws or state laws. To the extent this policy conflicts with the applicable requirements of the HIPAA Breach Notification Rule, the Breach Notification Rule shall govern.

DEFINITIONS

Except as otherwise described in this policy, all terms used shall have the definition given to them by the HIPAA Privacy, Security and Breach Notification Rules, as applicable.

Breach – The acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI. A breach does not include:

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if the 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 the HIPAA Privacy Rule;
- Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, and the information received is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or
- A disclosure of PHI 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.

An impermissible use or disclosure that does not fall under one of the three exceptions listed above is presumed to be a breach unless the covered entity or business associate demonstrates through a risk assessment that there is a low probability that the PHI has been compromised. This risk assessment must be based on at least the following four factors:

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

Additional factors may also need to be considered based on the circumstances of the impermissible use or disclosure.

Protected health information (PHI) – Information that is created or received by (or on behalf of) the Health Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. For purposes of this Privacy Policy, PHI does not include:

- Summary health information that is disclosed to the Plan Sponsor for the purpose of obtaining premium bids, or modifying, amending or terminating the Health Plan;
- Enrollment and disenrollment information for the Health Plan;
- PHI that is disclosed to the Health Plan or the Plan Sponsor pursuant to a valid HIPAA authorization; and
- Employment records that are created or received by the Plan Sponsor in its role as an employer, and not as a sponsor of the Health Plan.

Unsecured PHI – PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS. HHS designated encryption and destruction as the technologies and methodologies for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals.

COMPLIANCE REQUIREMENTS

The Plan Sponsor, on behalf of the Health Plan, shall investigate any incident that may constitute a breach of unsecured PHI and determine whether an impermissible use or disclosure has occurred. The Plan Sponsor will presume that an impermissible use or disclosure is a breach unless the Plan Sponsor's risk assessment demonstrates that there is a low probability that the PHI has been compromised. If the risk assessment does not show a low probability, the Plan Sponsor shall comply with the notification requirements as described below.

To Individuals

Following the discovery of a breach of unsecured PHI, the Plan Sponsor, on behalf of the Health Plan, shall notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of the breach. This notification must be made without unreasonable delay and no later than 60 calendar days of discovery of the breach.

To the Media

Following the discovery of a breach of unsecured PHI involving more than 500 residents of a state or jurisdiction, the Plan Sponsor, on behalf of the Health Plan, shall notify prominent media outlets serving the state or jurisdiction, in the form of a press release, at the same time notice is made to the individuals.

To HHS

Following a discovery of a breach of unsecured PHI, the Plan Sponsor, on behalf of the Health Plan, shall notify HHS as follows:

- For breaches of unsecured PHI involving 500 or more individuals, this notification will be provided to HHS at the same time notice is made to the individuals.

- For breaches of unsecured PHI involving fewer than 500 individuals, the Plan Sponsor shall maintain a log or other documentation of such breaches and, no later than 60 days after the end of each calendar year, provide the notification as instructed by HHS for breaches occurring during the previous calendar year.

Content of Notification

The notice of a breach of unsecured PHI shall be written in plain language and, to the extent possible, shall include the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI that were involved in the breach, such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved;
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the Health Plan is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an email address, website or postal address.

Method of Notification to Individuals

Notification to the media and to HHS shall be made as indicated in the applicable sections above. Notification to individuals shall be made as follows:

- **Written notice**—Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available. If the Health Plan knows the individual is deceased and has the address of the individual's next of kin or personal representative, written notification by first-class mail to the next of kin or personal representative.
- **Substitute notice**—In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
    - In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone or other means.
    - In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the homepage of the Health Plan's website, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside and shall include a toll-free phone number that remains active for at least 90 days where an individual can learn whether their unsecured PHI may be included in the breach.
- **Notice in urgent situations**—In any case deemed by the Health Plan to require urgency because of possible imminent misuse of unsecured PHI, the Health Plan may provide information to individuals by telephone or other means, as appropriate, in addition to written or substitute notice.

BREACHES OF UNSECURED PHI HELD BY BUSINESS ASSOCIATES

Any business associate of the Health Plan that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHI shall be required to notify the Health Plan of a breach of unsecured PHI without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. The notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired or disclosed during the breach. The business associate shall provide the Health Plan with any other information that the Health Plan is required to include in notification to the individual at the time of the notification (or promptly thereafter as information becomes available).

Upon receiving notification of a breach from a business associate, the Health Plan shall be responsible for notifying affected individuals, unless the Covered Entity and business associate otherwise agree that the business associate will provide such notice.

WORKFORCE TRAINING

The Plan Sponsor shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained on to how to identify and report breaches of unsecured PHI.

COMPLAINTS

The Plan Sponsor shall provide a process for individuals to make complaints regarding the Health Plan's PHI policies and procedures, its compliance with those policies and procedures, and its breach notification processes.

SANCTIONS

The Health Plan shall apply appropriate sanctions against members of its workforce who fail to comply with its privacy policies and procedures.

RETALIATION/WAIVER

The Health Plan shall not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The Health Plan may not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits.

SAMPLE HIPAA DOCUMENTS

IMPORTANT – CUSTOMIZATION REQUIRED

The following are sample documents for various HIPAA documentation requirements, such as the plan amendment and business associate agreement requirements. These samples cannot be used "as is"—they **must be customized** where indicated for specific plan and employer information. Also, if the sample policies do not accurately reflect an employer's implementation of the HIPAA Rules, they should be customized for the employer's specific approach. We encourage all customization to take place in coordination with knowledgeable benefits counsel.

Nothing in this toolkit should be considered as legal advice, including these sample documents. These sample documents are provided for educational and illustrative purposes only.

SAMPLE HEALTH PLAN AMENDMENT

The **[Insert Group Health Plan Name]** (Plan) is a group health plan sponsored by **[Insert Company Name]** (Plan Sponsor). The Plan Sponsor has access to protected health information (PHI) for certain administration functions for the Plan. The Plan Sponsor shall have access to PHI only as permitted under this Amendment or as otherwise required or permitted by HIPAA.

Protected Health Information

PHI means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of an individual; 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 that identifies the individual or for which there is a reasonable basis to believe that the information can be used to identify the individual. PHI includes information in any form, including electronic PHI (ePHI). It does not include health information about an employee that is held in the Plan Sponsor's employment records in its role as an employer

Permitted Disclosures

Enrollment information: The Plan, or a health insurance issuer or HMO for the Plan, may disclose to the Plan Sponsor information on whether an individual is participating in the Plan, or is enrolled in or has disenrolled from the health insurance or HMO offered by the Plan, in accordance with 45 CFR §164.504(f)(1)(iii).

Summary health information: In accordance with 45 CFR §164.504(f)(1)(ii), the Plan (or the issuer or HMO with respect to the Plan) may disclose summary health information to the Plan Sponsor if the Plan Sponsor requests the information for the purposes of (1) obtaining premium bids from health plans for providing health insurance coverage under the Plan; or (2) modifying, amending or terminating the Plan.

Summary health information means information (1) that summarizes the claims history, claims expenses or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under the Plan; and (2) from which the information described at 45 CFR §164.514(b)(2)(i) has been deleted, except that the geographic information described in 45 CFR §164.514(b)(2)(i)(B) need only be aggregated to the level of a five-digit ZIP code.

Valid HIPAA authorization: The Plan (or the issuer or HMO with respect to the Plan) may also disclose PHI to the Plan Sponsor pursuant to a signed authorization that meets the requirements of 45 CFR §164.508(b)(1).

Disclosures for Plan Administration Purposes

The Plan (or the issuer or HMO with respect to the Plan) may disclose PHI to the Plan Sponsor for plan administration purposes. Plan administration purposes means administration functions performed by the Plan Sponsor on behalf of the Plan, such as claims processing, coordination of benefits, quality assurance, auditing and monitoring. Plan administration purposes do not include functions performed by the Plan Sponsor in connection with any other benefit or benefit plan of the Plan Sponsor or any employment-related actions or decisions.

The Plan Sponsor agrees that with respect to any PHI (other than enrollment/disenrollment information, summary health information and information disclosed pursuant to a valid HIPAA authorization) disclosed to it by the Plan (or the issuer or HMO for the Plan) the Plan Sponsor will:

- Not use or further disclose the information other than as permitted or required by the Plan or as required by law;
- Ensure that any agents, including subcontractors, to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to PHI;
- Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor;

- Report to the Plan any use or disclosure of PHI of which it becomes aware that is inconsistent with the permissible uses or disclosures;
- Make PHI available in accordance with the individual rights under 45 CFR §164.524;
- Make an individual's PHI available for amendment, and incorporate any amendments, as required under 45 CFR §164.526;
- Make available the information required to provide an accounting of disclosures to individuals, as required under 45 CFR §164.528;
- Make its internal practices, books and records relating to the use and disclosure of PHI received from the HIPAA Plans available to the Secretary of the Department of Health and Human Services for purposes of determining compliance with HIPAA's requirements;
- If feasible, return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and retain no copies of this information when no longer needed for the purpose for which disclosure was made, except that, if this return or destruction is not feasible, limit further uses or disclosures to those purposes that make the return or destruction of the information infeasible; and
- Ensure adequate separation between the Plan and the Plan Sponsor is established.

The Plan (or the issuer or HMO with respect to the Plan) will disclose PHI to the Plan Sponsor for plan administration purposes only upon receipt of a certification that the plan documents have been amended to include the protections listed above.

Adequate Separation

Only those employees or classes of employees identified in the Plan's HIPAA policies may have access to and use and disclose PHI for plan administration purposes. Any employee who violates the terms of this Amendment, or the Plan Sponsor's HIPAA policies, shall be subject to the Plan Sponsor's sanctions policy for HIPAA violations.

Security

The Plan Sponsor will reasonably and appropriately safeguard ePHI (other than enrollment/disenrollment information, summary health information and information disclosed pursuant to a valid HIPAA authorization) that is created, received, maintained, or transmitted to or by the Plan Sponsor on behalf of the Plan. The Plan Sponsor will:

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains or transmits on behalf of the HIPAA Plan;
- Ensure that adequate separation between the HIPAA Plans and the Plan Sponsor is supported by reasonable and appropriate security measures;
- Ensure that any agent, including a subcontractor, to whom it provides ePHI agrees to implement reasonable and appropriate security measures to protect the information; and
- Report to the Plan any security incident of which it becomes aware.

This Plan Amendment shall take effect the _____ day of _____, 20___, and has been adopted on behalf of the Plan Sponsor by:

_____

Signature

_____

Printed Name and Title

_____

Date

SAMPLE PLAN SPONSOR CERTIFICATION

[Insert Company Name] (Plan Sponsor), the sponsor of the **[Insert Group Health Plan Name]** (Plan), certifies pursuant to 45 CFR §164.504(f)(2)(ii) that the Plan has been amended to incorporate the following provisions and the Plan Sponsor agrees to:

- Not use or further disclose protected health information (PHI) other than as permitted or required by the Plan or as required by law;
- Ensure that any agents, including subcontractors, to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to PHI;
- Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor;
- Report to the Plan any use or disclosure of PHI of which it becomes aware that is inconsistent with the permissible uses or disclosures;
- Make PHI available in accordance with the individual rights under 45 CFR §164.524;
- Make an individual's PHI available for amendment, and incorporate any amendments, as required under 45 CFR §164.526;
- Make available the information required to provide an accounting of disclosures to individuals, as required under 45 CFR §164.528;
- Make its internal practices, books and records relating to the use and disclosure of PHI received from the HIPAA Plans available to the Secretary of the Department of Health and Human Services for purposes of determining compliance with HIPAA's requirements;
- If feasible, return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and retain no copies of this information when no longer needed for the purpose for which disclosure was made, except that, if this return or destruction is not feasible, limit further uses or disclosures to those purposes that make the return or destruction of the information infeasible; and
- Ensure adequate separation between the Plan and the Plan Sponsor is established.

_____ _____

Signature Date

_____

Printed Name and Title

SAMPLE BUSINESS ASSOCATION AGREEMENT

This Business Associate Contract (Agreement) is entered into by and between **[Insert Company Name]**, on behalf of **[Insert Group Health Plan Name]** (Covered Entity), and **[Insert Service Provider Name]** (Business Associate), effective as of **[Insert Effective Date]**.

WHEREAS, Covered Entity is a group health plan, as defined under the Health Insurance Portability and Accountability Act of 1996 and related regulations promulgated by the U.S. Department of Health and Human Services (HHS) (collectively, HIPAA), which is sponsored and maintained by the Company.

WHEREAS, Business Associate is a business associate of Covered Entity, as defined in the HIPAA Privacy, Security, Breach Notification and Enforcement Rules (HIPAA Rules) at 45 CFR 160.103.

WHEREAS, Business Associate may access, use, create, maintain, transmit, receive and/or disclose Protected Health Information (PHI) on behalf of Covered Entity.

WHEREAS, pursuant to the HIPAA Rules, the Business Associate must agree in writing to comply with the obligations required of business associates by the HIPAA Rules.

NOW, THEREFORE, in consideration of the mutual promises set forth below, the parties hereby agree as follows:

A. DEFINITIONS

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Rules at 45 CFR Part 160 and 164.

B. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

Business Associate agrees to:

1. Not use or further disclose PHI other than as permitted or required by the Agreement or as required by law.
2. Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent the use or disclosure of PHI other than provided for by the Agreement.
3. Report to Covered Entity any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including breaches of unsecured PHI as required by 45 CFR 164.410 and any security incident of which it becomes aware.
4. Ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate agree to the same restrictions, conditions and requirements that apply to Business Associate with respect to such information, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable.
5. Make available PHI in a designated record set to Covered Entity as necessary to meet the requirements under 45 CFR 164.524. Make any amendment(s) to PHI in a designated record set as directed or agreed to by Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526. This provision shall not be applicable if Business Associate does maintain PHI in a designated record set.
6. Maintain and make available the information required to make an accounting of disclosures to Covered Entity, as necessary to satisfy Covered Entity's obligations under 45 CFR Section 164.528.
7. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).
8. Make its internal practices, books and records available to the Secretary of HHS for the purpose of determining compliance with the HIPAA Rules.

C. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

1. Business Associate may only use or disclose PHI as necessary to provide the services described in its underlying service agreement with the Company or for other purposes permitted or required of Business Associate by the Agreement.
2. Business Associate may use or disclose PHI as required by law.
3. Business Associate agrees to make uses and disclosures and requests for PHI consistent with Covered Entity's minimum necessary policies and procedures.
4. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth below.
5. Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
6. Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the disclosures are required by law or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
7. Business Associate may provide data aggregation services relating to the health care operations of Covered Entity.

D. OBLIGATIONS OF COVERED ENTITY

1. Covered Entity shall comply with each applicable requirement of the HIPAA Rules.
2. Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR Section 164.520 to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
3. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose their PHI to the extent that such changes may affect Business Associate's use and disclosure of PHI.
4. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR Section 164.522 to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

E. PERMISSIBLE REQUESTS BY COVERED ENTITY

Except for data aggregation or the management and administration and legal responsibilities of Business Associate, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

F. TERM AND TERMINATION

1. The term of the Agreement shall begin on the Effective Date and shall remain in effect until the underlying service agreement between the Company and Business Associate terminates or the Agreement is terminated under Section F(2) of the Agreement, whichever is sooner.

2. This Agreement shall be terminated only as follows:

    a. Termination for Cause by Covered Entity: The Agreement may be terminated by Covered Entity upon fifteen (15) days advance written notice to Business Associate if Covered Entity determines that Business Associate has violated a material term of the Agreement and Business Associate does not cure the breach or end the violation within such fifteen (15)-day period.

b. Termination for Cause by Business Associate: The Agreement may be terminated by Business Associate upon fifteen (15) days advance written notice to Covered Entity if Business Associate determines that Covered Entity has violated a material term of the Agreement and Covered Entity does not cure the breach or end the violation within such fifteen (15)-day period.

c. Termination Due to Change in Law: Either party may terminate the Agreement effective upon thirty (30) days advance written notice to the other party in the event that the terminating party has sought amendment of this Agreement pursuant to Section G(2) of the Agreement, and no amendment has been agreed upon.

3. Upon termination of the Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity or created, maintained or received by Business Associate on behalf of Covered Entity, shall:

   a. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

   b. Return to Covered Entity or destroy the remaining PHI that Business Associate still maintains in any form;

   c. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

   d. Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out in Section C, which applied prior to termination; and

   e. Return to Covered Entity or destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

4. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

G. GENERAL PROVISIONS

1. A reference in the Agreement to a section in the HIPAA Rules means the section as in effect or as amended.
2. The Agreement may be amended only by the mutual written agreement of the parties. The parties agree to take such action to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable laws.
3. The Agreement shall be construed and enforced in accordance with the laws of the State that governs the underlying agreement between the Company and Business Associate.
4. Neither this Agreement nor any of the rights, benefits, duties, or obligations provided herein may be assigned by any party to this Agreement without the prior written consent of the other party.
5. Nothing in this Agreement shall be deemed to create any rights or remedies for any third party.
6. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.
7. Any notice given under this Agreement must be in writing and delivered via first class mail, via reputable overnight courier service, or in person to the parties' respective addresses as specified in the underlying service agreement or to such other address as the parties may from time to time designate in writing.

IN WITNESS WHEREOF, the undersigned have executed this Agreement.

Plan Sponsor (on behalf of Covered Entity)

_____
Signature

_____
Date

_____
Name

_____
Title

Business Associate

_____
Signature

_____
Date

_____
Name

_____
Title

SAMPLE NOTICE OF PRIVACY PRACTICES

Special Notes

The Department of Health and Human Services (HHS) maintains model notices of privacy practices (Privacy Notices) for health plans and health care providers. HHS has **three different formatted options** for the Privacy Notice for health plans, as well as a text only option, in both English and Spanish. These formatted options are provided as fillable PDF files. All of the model notices, as well as instructions for using the models, are available on HHS' website at: www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html. Below is HHS' text-only option for a health plan's Privacy Notice.

*The model notices have not been updated to include the new privacy rights for reproductive health care. The deadline for covered entities to update their Privacy Notices for these new rights is **Feb. 16, 2026**. It is expected that HHS will update its model notices to incorporate the new requirements before the compliance deadline.*

Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. **Please review it carefully.**

YOUR RIGHTS

You have the right to:

- Get a copy of your health and claims records.
- Correct your health and claims records.
- Request confidential communication.
- Ask us to limit the information we share.
- Get a list of those with whom we've shared your information.
- Get a copy of this privacy notice.
- Choose someone to act for you.
- File a complaint if you believe your privacy rights have been violated.

YOUR CHOICES

You have some choices in the way that we use and share information as we:

- Answer coverage questions from your family and friends.
- Provide disaster relief.
- Market our services and sell your information.

OUR USES AND DISCLOSURES

We may use and share your information as we:

- Help manage the health care treatment you receive.
- Run our organization.
- Pay for your health services.
- Administer your health plan.
- Help with public health and safety issues.
- Do research.

- Comply with the law.
- Respond to organ and tissue donation requests and work with a medical examiner or funeral director.
- Address workers' compensation, law enforcement and other government requests.
- Respond to lawsuits and legal actions.

YOUR RIGHTS

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get a copy of health and claims records.

- You can ask to see or get a copy of your health and claims records and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health and claims records, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

Ask us to correct health and claims records.

- You can ask us to correct your health and claims records if you think they are incorrect or incomplete. Ask us how to do this.
- We may say "no" to your request, but we'll tell you why in writing within 60 days.

Request confidential communications.

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will consider all reasonable requests, and must say "yes" if you tell us you would be in danger if we do not.

Ask us to limit what we use or share.

- You can ask us not to use or share certain health information for treatment, payment or our operations.
- We are not required to agree to your request, and we may say "no" if it would affect your care.

Get a list of those with whom we've shared information.

- You can ask for a list (accounting) of the times we've shared your health information for six years prior to the date you ask, who we shared it with and why.
- We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We'll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

Get a copy of this privacy notice.

- You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

Choose someone to act for you.

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
- We will make sure the person has this authority and can act for you before we take any action.

File a complaint if you feel your rights are violated.

- You can complain if you feel we have violated your rights by contacting us using the information on Page 1.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775 or visiting **www.hhs.gov/ocr/privacy/hipaa/complaints/**.
- We will not retaliate against you for filing a complaint.

YOUR CHOICES

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:

- Share information with your family, close friends or others involved in payment for your care.
- Share information in a disaster relief situation.

If you are not able to tell us your preference, for example, if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases, we **never** share your information unless you give us written permission:

- Marketing purposes
- Sale of your information

OUR USES AND DISCLOSURES

How do we typically use or share your health information?

We typically use or share your health information in the following ways.

Help manage the health care treatment you receive.

- We can use your health information and share it with professionals who are treating you.

Example: A doctor sends us information about your diagnosis and treatment plan so we can arrange additional services.

Run our organization.

- We can use and disclose your information to run our organization and contact you when necessary.
- We are not allowed to use genetic information to decide whether we will give you coverage and the price of that coverage. This does not apply to long-term care plans.

Example: We use health information about you to develop better services for you.

Pay for your health services.

- We can use and disclose your health information as we pay for your health services.

Example: We share information about you with your dental plan to coordinate payment for your dental work.

Administer your plan.

- We may disclose your health information to your health plan sponsor for plan administration.

Example: Your company contracts with us to provide a health plan, and we provide your company with certain statistics to explain the premiums we charge.

How else can we use or share your health information?

We are allowed or required to share your information in other ways—usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes. For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html**.**

Help with public health and safety issues.

- We can share health information about you for certain situations such as:
  - Preventing disease
  - Helping with product recalls
  - Reporting adverse reactions to medications
  - Reporting suspected abuse, neglect or domestic violence
  - Preventing or reducing a serious threat to anyone's health or safety

Do research.

- We can use or share your information for health research.

Comply with the law.

- We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.

Respond to organ and tissue donation requests, and work with a medical examiner or funeral director.

- We can share health information about you with organ procurement organizations.
- We can share health information with a coroner, medical examiner or funeral director when an individual dies.

Address workers' compensation, law enforcement and other government requests.

- We can use or share health information about you:
  - For workers' compensation claims
  - For law enforcement purposes or with a law enforcement official
  - With health oversight agencies for activities authorized by law
  - For special government functions such as military, national security and presidential protective services

OUR RESPONSIBILITIES

Respond to lawsuits and legal actions.

- We can share health information about you in response to a court or administrative order, or in response to a subpoena.
  - We are required by law to maintain the privacy and security of your protected health information.
  - We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
  - We must follow the duties and privacy practices described in this notice and give you a copy of it.

- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.

CHANGES TO THE TERMS OF THIS NOTICE

We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, on our website, and we will mail a copy to you.

OTHER INSTRUCTIONS FOR NOTICE

- [Insert effective date of this Notice.]
- [Insert name or title of the privacy official (or other privacy contact) and their email address and phone number.]
- [Insert any special notes that apply to your entity's practices, such as "we do not create or manage a hospital directory" or "we do not create or maintain psychotherapy notes at this practice."]
- [The Privacy Rule requires you to describe any state or other laws that require greater limits on disclosures. For example, "We will never share any substance abuse treatment records without your written permission." Insert this type of information here. If no laws with greater limits apply to your entity, no information needs to be added.]
- [If your entity provides patients with access to their health information via the Blue Button protocol, you may want to insert a reference to it here.]
- [If your entity is part of an organized health care arrangement (OHCA) that has agreed to a joint notice, use this space to inform your patients of how you share information within the OHCA (such as for treatment, payment and operations related to the OHCA). Also, describe the other entities covered by this notice and their service locations. For example, "This notice applies to Grace Community Hospitals and Emergency Services Incorporated which operate the emergency services within all Grace hospitals in the greater Dayton area."]

SAMPLE NOTICE OF AVAILABILITY OF PRIVACY NOTICE (SELF-INSURED HEALTH PLANS)

[Insert Date]

[Insert Employee Name]

[Insert Employee Address]

[Insert City, State and ZIP code]

RE: Notice of Availability of HIPAA Privacy Notice

Dear **[Insert employee name]**,

The **[Insert Name of Group Health Plan]** (Plan) maintains a Notice of Privacy Practices (Privacy Notice) that explains how the Plan uses and discloses protected health information (PHI) and your rights and the Plan's legal duties with respect to PHI. If you would like to receive a copy of the Plan's Privacy Notice, please contact **[Insert contact information]** to request a copy.

Sincerely,

[Insert name]

[Insert title]

SAMPLE HIPAA AUTHORIZATION

I authorize the use and disclosure of protected health information as described below.

Participant name: _____

Person/entity authorized to use and disclose the information:
_____

Person/entity authorized to receive and use the information:
_____

Expiration date or event: _____

Specific description of the information that is to be used or disclosed (including relevant dates and conditions):

Purpose of the use or disclosure:

I understand that:

- Signing this authorization is voluntary and I may refuse to sign it.
- If I refuse to sign this form, it will not impact treatment or payment for health care, or enrollment or eligibility for benefits under a health plan.
- Once this information is disclosed, it may be redisclosed by the recipient and no longer protected by federal privacy regulations.
- I may revoke this authorization at any time by sending a written revocation to the entity designated above as being authorized to use or disclose protected health information. I also understand that my revocation will not apply to uses and disclosures made before the revocation is received by the entity.

Signature of Participant (or Personal Representative): _____

Date: _____

If this form is completed by a personal representative, complete the following information:

Name of Personal Representative (printed): _____

Relationship to Participant and Authority Status:_____

MODEL ATTESTATION FOR A REQUESTED USE OR DISCLOSURE OF PHI POTENTIALLY RELATED TO REPRODUCTIVE HEALTH CARE

Special Notes

New protections for reproductive health care privacy become effective on Dec. 23, 2024. These new protections require covered entities and business associates to obtain a valid attestation before using or disclosing PHI potentially related to reproductive health care for certain purposes, such as health oversight activities and judicial or administrative proceedings. HHS has provided the following model attestation form that covered entities and business associates may use to comply with new protections for reproductive health care privacy. This model form also includes background information and instructions for its use.

Background Information

When a HIPAA covered entity or business associate receives a request for protected health information (PHI) potentially related to reproductive health care, it must obtain a signed attestation that clearly states the requested use or disclosure is not for the prohibited purposes described below, where the request is for PHI for any of the following purposes:

- Health oversight activities
- Judicial or administrative proceedings
- Law enforcement
- Regarding decedents, disclosures to coroners and medical examiners

Prohibited Purposes. Covered entities and their business associates may not use or disclose PHI for the following purposes:

a. To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care.

b. To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care.

c. To identify any person for any purpose described in (1) or (2).

The prohibition applies when the reproductive health care at issue (1) is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided, (2) is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which such health care is provided, regardless of the state in which it is provided, or (3) is provided by another person and presumed lawful.

Model Instructions

Information for the Person Requesting the PHI

- By signing this attestation, you are verifying that you are not requesting PHI for a prohibited purpose and acknowledging that criminal penalties may apply if untrue.

- You may not add content that is not required or combine this form with another document except where another document is needed to support your statement that the requested disclosure is not for a prohibited purpose. For

example, if the requested PHI is potentially related to reproductive health care that was provided by someone other than the covered entity or business associate from whom you are requesting the PHI, you may submit a document that supplies information that demonstrates a substantial factual basis that the reproductive health care in question was not lawful under the specific circumstances in which it was provided.

Information for the Covered Entity or Business Associate

- You may not rely on the attestation to disclose the requested PHI if any of the following is true:
    - It is missing any required element or statement or contains other content that is not required.
    - It is combined with other documents, except for documents provided to support the attestation.
    - You know that material information in the attestation is false.
    - A reasonable covered entity or business associate in the same position would not believe the requestor's statement that the use or disclosure is not for a prohibited purpose as described above.
- If you later discover information that reasonably shows that any representation made in the attestation is materially false, leading to a use or disclosure for a prohibited purpose as described above, you must stop making the requested use or disclosure.
- You may not make a disclosure if the reproductive health care was provided by a person other than yourself and the requestor indicates that the PHI requested is for a prohibited purpose as described above, unless the requestor supplies information that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided.
- You must obtain a new attestation for each specific use or disclosure request.
- You must maintain a written copy of the completed attestation and any relevant supporting documents.

Model Attestation Regarding a Requested Use or Disclosure of Protected Health Information Potentially Related to Reproductive Health Care

The entire form must be completed for the attestation to be valid.

Name of person(s) or specific identification of the class of persons to receive the requested PHI.
e.g., name of investigator and/or agency making the request
Name or other specific identification of the person or class of persons from whom you are requesting the use or disclosure.
e.g., name of covered entity or business associate that maintains the PHI and/or name of their workforce member who handles requests for PHI
Description of specific PHI requested, including name(s) of individual(s), if practicable, or a description of the class of individuals, whose protected health information you are requesting.
e.g., visit summary for [name of individual] on [date]; list of individuals who obtained [name of prescription medication] between [date range]

I attest that the use or disclosure of PHI that I am requesting is not for a purpose prohibited by the HIPAA Privacy Rule at 45 CFR 164.502(a)(5)(iii) because of one of the following (check one box):

☐ The purpose of the use or disclosure of protected health information is **not** to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care or to identify any person for such purposes.

☐ The purpose of the use or disclosure of protected health information **is** to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, or to identify any person for such purposes, but the reproductive health care at issue was **not lawful** under the circumstances in which it was provided.

I understand that I may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if I knowingly and in violation of HIPAA obtain individually identifiable health information relating to an individual or disclose individually identifiable health information to another person.

Signature of the person requesting the PHI

_____ Date _____

If you have signed as a representative of the person requesting PHI*, provide a description of your authority to act for that person.*

_____

This attestation document may be provided in electronic format, and electronically signed by the person requesting protected health information when the electronic signature is valid under applicable Federal and state law.