Guide to Employers

HIPAA Privacy and Security Rules

The federal Health Insurance Portability and Accountability Act (HIPAA) covers a wide range of health coverage issues. It includes provisions for portability of coverage, protections for small employers that purchase group insurance, and prohibitions against discrimination based on an individual's health status.

HIPAA also includes a complex set of rules related to the privacy and security of an individual's protected health information (PHI):

- The **Privacy Rule** sets standards for the use and disclosure of PHI as well as standards for the individual's right to understand and control how their information is used. Health plans must establish policies and procedures to protect PHI, ensure its staff is trained on the rules, and provide notices to individuals explaining their privacy rights.
- The **Security Rule** sets security standards to safeguard and protect PHI that is stored or transferred in electronic form. Requirements include physical, technical, and administrative safeguards. In the event of a security breach, the Plan must notify all affected persons, report the breach to the government and, in some cases, notify the media.

The U.S. Department of Health and Human Services (HHS) regulates and enforces the Privacy Rule and Security Rule through its Office for Civil Rights (OCR).

This guide reviews key features of the Privacy Rule and Security Rule ("the Rules") specifically for employers that sponsor group health plans:

- Quick Facts
- The Rules in Brief
- The Employer's Role
- Privacy Notices
- Business Associate Agreements
- HIPAA Authorizations
- Breaches
- Penalties
- Employer Checklist
- Sample Materials

This guide offers general information based on federal regulations and guidance as of September 2017. The guide pertains to employers solely in their role as group health plan sponsors. Employers that also are health care providers, such as hospitals and medical groups, are not addressed. Legal advice is not provided nor intended. Similar to most federal health-related laws, the HIPAA Privacy Rule and Security Rule are extremely complex and all employers are advised to review their unique situation and health plan requirements with experienced legal counsel.

Quick Facts

This guide covers the Rules for group health plans only

The Rules apply to **covered entities**:

- Health care providers;
- Health care clearinghouses; and
- Health care plans

Employers are not covered entities and the Rules do not apply to employers directly. As group health plan sponsors, however, employers are responsible for their plan's compliance with the Rules.

The extent of the employer's duties depends on whether its group health plan is insured or self-funded and whether the employer has access to protected health information (PHI) for plan administration.

The Rules also apply to **business associates;** i.e., third parties or subcontractors that perform services for the health plan involving the use of PHI. Examples include:

- Third-party administrators, pharmacy benefit managers, and wellness program vendors;
- Legal, actuarial, data aggregation, financial, and other service providers; and
- Brokers and consultants.

An insurer, that is the carrier insuring the health plan, is not a business associate. A health insurer is a covered entity in its own right.

A **health plan** is a plan or program that provides or pays the cost of health care, including insured and self-funded group health plans. So-called "excepted benefits," such as limited-scope dental and vision plans, employee assistance programs (EAPs), and health flexible spending accounts (HFSAs), are not exempt from the Rules.

A narrow exception applies to self-funded self-administered plans with fewer than 50 eligible employees. This is uncommon.

The Rules do not apply to non-health plans or arrangements, such as life or accident insurance, disability income benefits, or workers' compensation. Also, the Rules do not apply to on-site clinics as health plans (although they may be subject to the Rules as health care providers) and do not apply to health savings accounts (HSAs).

Protected health information (PHI) is oral, written, or electronic health information that is:

- Individually identifiable;
- Created, received, stored, or transmitted by the health plan; and
- Related to:
  - An individual's past, present, or future physical or mental health or condition;
  - Providing health care to the individual; or
  - Past, present, or future payment for providing health care to the individual.

The Rules do not apply to **de-identified information**. Information is presumed to be de-identified if 18 specific identifiers (such as names, ID numbers of any kind) are removed and the information cannot be used, alone or in combination with other information, to identify the individual.

Lastly, the Rules do not apply to information, even if individually-identifiable, that does not move through a health plan. Examples include pre-employment screens, sick leave requests, FMLA requests, and return-to-work notes. Although not directly subject to HIPAA, employers nonetheless are advised to safeguard all information as confidential and allow access only to staff with a need to know.

The Rules in Brief

The Rules govern how health plans are allowed to use and disclose PHI. Some uses are permitted without the individual's authorization, either for plan administration purposes or to meet public health and law enforcement needs. Other uses are not permitted unless the individual has given his or her permission by means of a HIPAA Authorization.

Plans must establish and maintain safeguards against unauthorized use or disclosure of PHI, protect against security threats, and ensure compliance by employees that perform functions on the plan's behalf (called the plan's workforce).

The key provisions for health plans are summarized here. The employer sponsoring the health plan may be responsible for a few, or for many, of the provisions depending on the type of plan and administration. We review the different types of employer responsibilities in the next section. This section offers highlights of the rules in general.

The Rules have four basic types of requirements:

- Use and Disclosure Provisions;
- Individual Rights;
- Administrative Safeguards; and
- Security Rule (with respect to electronic PHI)

Use and Disclosure Provisions

Treatment, Payment, and Operations (TPO). The Plan may use and disclose PHI for purposes of treatment, payment, and operations (TPO) without a HIPAA Authorization, provided the Plan:

- Identifies the employees designated to access PHI (i.e., the Plan's workforce);
- Allows only the minimum necessary PHI to be used or disclosed; and
- Ensures that the recipient of the disclosed PHI is entitled to receive it for the stated purpose.

Legal disclosures. The Plan also may disclose PHI without a HIPAA Authorization if required by law. Examples include:

- Disclosures for workers' compensation;
- Court orders and subpoenas;
- Judicial and administrative proceedings; and
- Public health activities.

HIPAA Authorization. The Plan may use and disclose an individual's PHI to the extent the individual has authorized. A valid HIPAA Authorization must meet several criteria. See page 9 for discussion.

Individual Rights

The Rules require the Plan to grant certain rights to individuals. With respect to his or her PHI, each individual may request:

- Copies of PHI for review, either in hard copy or electronically;
- Amendments or changes to PHI;
- Accounting of certain disclosures of PHI;
- Confidential communications; and
- Restrictions.

Administrative Safeguards

The Rules impose extensive administrative requirements which are intended to safeguard PHI. The Plan must:

- Establish written policies and procedures for uses and disclosures and limiting access to PHI;
- Designate a Privacy Officer and Security Officer (most plans also designate a Privacy Contact for routine matters);
- Ensure plan documents, notices of privacy practices, and other materials are compliant;
- Obtain business associate agreements with any third-party administrators, vendors, brokers, or others who will have access to PHI;
- Establish policies for securing information, implementing physical safeguards (such as locked doors and cabinets), and evaluating electronic safeguards; and
- Ensure employees with access to PHI are properly trained on the Plan's policies and procedures.

Security Rule

The Security Rule imposes requirements to protect electronic PHI, which generally is any PHI that is not either handwritten or oral. Even hard copy PHI likely has been created or stored using electronic media.

There are five categories of standards, including administrative, physical, technical, organizational, and documentation requirements. To ensure compliance, the Plan must perform a risk analysis to identify and implement appropriate standards and document the steps its take to meet each standard. The entity's information technology (IT) professionals usually take the lead with these requirements, which are detailed and complex.

The next section reviews how the Rules affect employers that sponsor group health plans. Later sections provide details and sample materials for items that often generate questions from employers: Privacy Notices, Business Associate Agreements, HIPAA Authorizations, and Breach Notifications.

The Employer's Role

The Rules do not apply directly to employers but any employer that sponsors a group health plan is responsible for certain duties on behalf of its plan. The scope of the employer's responsibilities will vary depending on the type of plan and whether the employer has access to PHI.

Employer Type A: (Insured/Hands-Off Approach)

- All plans are insured; that is all coverages are provided through group insurance contracts (including HMO contracts); and
- Employer does not create or receive PHI except for summary health information and/or enrollment forms. (Summary health information contains no individually identifiable information; for example, de-identified claims report. The employer may receive it from the carrier for purposes of obtaining bids or amending or terminating the plan.)

The employer's duties are simple (and should be common practice):

- Refrain from retaliating against plan participant who alleges a violation of the Rules; and
- Do not condition enrollment or eligibility for benefits, treatment, or payment on the individual's waiver of his or her privacy rights.

To continue as Type A, the employer must avoid creating or receiving PHI. For instance, do not assist employees with claim issues. If the employer sends or receives enrollment data electronically, additional duties will apply.

Employer Type B: (Insured/Hands-On Approach)

- Plan is insured; and
- Employer creates or receives PHI that is not merely health summary information or enrollment forms. Examples include managing carve-out plans, certain wellness activities, and assisting with claims issues.

Identify the Workforce and Build a Firewall
The Plan's workforce are specific employees (usually in HR, Benefits, and IT) who perform tasks for the Plan. The workforce may use PHI, if done according to the Rules, but everyone else must be walled off.

The Plan may disclose PHI to the plan sponsor (employer) provided:

- Plan document is amended to allow the plan sponsor to have access to PHI for purposes of plan administration; and
- Plan sponsor certifies that document is amended and agrees to terms and conditions in the amendment (for example limits on uses, description of workforce, firewall).

The Type B employer must comply with numerous Rules. See Employer Checklist on page 13.

Employer Type C: (Self-funded/Hands-On Approach)

Plan is self-funded by the employer. The employer is assumed to have access to PHI since the nature of a self-funded plan is that the employer has final authority for claim decisions.

In this case, the employer is responsible for the Plan's compliance with the Rules. See Employer Checklist on page 13.

On the following pages, we take a closer look at items that often generate questions from employers: Privacy Notices, Business Associate Agreements, HIPAA Authorizations, and Breach Notifications.

Privacy Notices

Health plans are required to distribute a Notice of Privacy Practices (Privacy Notice) to all Plan participants, including covered employees, retirees, and COBRA beneficiaries, that describes:

- The Plan's uses and disclosures of PHI; and
- The individual's rights:
  - To inspect and obtain a copy of his or her PHI;
  - To have the Plan amend PHI;
  - To request restrictions on certain disclosures of PHI;
  - To request confidential communications of PHI; and
  - To receive an accounting of disclosures of PHI made within the prior six years.

Who is Responsible for the Privacy Notice?

The Plan is responsible for maintaining and distributing a Privacy Notice. If the Plan is insured, that means the insurance company. If the employer has access to PHI, other than merely enrollment information for administration purposes, the employer also needs to create and distribute a notice. If, however, the employer's only access to PHI in an insured plan is for administration purposes, the employer does not need to create a notice but must distribute the carrier's notice if a participant requests it.
With respect to self-funded health plans, the employer is responsible for all requirements.

When is the Notice Distributed?

The Privacy Notice must be distributed to Plan participants:

- At the time of his or her initial enrollment in the Plan;
- Upon the individual's request; and
- Within 60 days of a material change in the content of the Notice.

Further, at least once every three years, the Plan must notify participants that the Privacy Notice is available and how to obtain a copy free of charge. The Plan may meet this requirement by distributing either the complete Privacy Notice or a short reminder notice.

How is the Notice Distributed?

Notices must be delivered to the intended recipients. Simply posting the notice on a website or workplace kiosk or bulletin board does not satisfy the distribution requirement.

- Notices can be included with other Plan materials, such as the new hire or open enrollment kit. It cannot be part of the same document as a HIPAA authorization.
- The notice can be delivered electronically (by email, for example) but only if the individual has provided his or her consent, including consenting to any hardware or software requirements and acknowledging that his or her consent to receive the notice electronically may be withdrawn at any time.

Electronic distribution is allowed, but the conditions are more restrictive than for other types of benefit notices.

- If the Plan maintains a website describing services and benefits, the notice must be posted there in addition to distribution to individuals.
- Separate distribution for dependents is not required, unless the Plan knows they have a different address from the employee or if the dependent requests the notice.

Samples:

For sample language for the Notice of Privacy Practices and the Reminder of Availability of the Notice of Privacy Practices, see the Sample Materials in this guide.

Business Associate Agreements (BAAs)

Health plans must receive satisfactory assurances from business associates that PHI will be handled and safeguarded appropriately. To do so, the Plan must enter into a contract, called a business associate agreement (BAA), with each business associate to establish the permitted and required uses and disclosures of PHI. The BAA also must require the business associate to:

- Implement appropriate safeguards (for example, limit access to employees on a need-to-know basis);
- Report to the health plan any known use or disclosure of PHI not permitted by the BAA 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 rules;
- Maintain an accounting of disclosures, made during the last six years, and make the accounting available upon request;
- Make its internal practices, books and records relating to use and disclosure of PHI available to the U.S. Department of Health and Human Services (HHS); and
- At termination, the business associate must destroy or return all PHI, if feasible, or extend the limitations on use and disclosure beyond termination of the contract.

Business associates are third parties (for example, TPAs, PBMs, brokers, and others) that use PHI to perform services for the health plan. Insurers, however, are not business associates as they are covered entities in their own right.

A business associate that uses a subcontractor is required to enter into a BAA with its subcontractor.

Note that most TPAs and service providers have developed BAAs for their clients' use. The employer should carefully review all language with its legal counsel before signing. The BAA may include provisions, such as hold harmless or indemnification clauses, not required by HIPAA.

For sample language for a Business Associate Agreement (BAA), see Sample Materials in this guide.

HIPAA Authorizations

Health plans may use and disclose PHI for purposes of treatment, payment, or healthcare operations (TPO events), or if required by law such as for public health or law enforcement. For any other purposes, however, the Plan first must obtain the individual's authorization. This is commonly called a HIPAA Authorization.

A HIPAA Authorization must be written in plain language and contain all of the following:

- Description of the information to be used or disclosed with enough specifics so the Plan knows what information the authorization pertains to;
- Name or other specific identification of the person or classes of persons that are authorized to release the PHI;
- Name or other specific identification of the person or classes of persons that are authorized to receive the PHI;
- Description of the purpose of the requested use or disclosure (at the request of the individual, for example);
- Date or event on which the authorization expires;
- Statement that the individual has a right to revoke the authorization in writing and information about how to make a revocation;
- Explanation of the Plan's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the receipt of an authorization; and
- 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 privacy rules.

Blanket or "catch-all" authorizations are not valid. Each authorization must specify the information to be used or disclosed and its purpose.

The authorization must be signed and dated by the individual. Alternatively, the individual's personal representative may sign the authorization provided that the representative indicates his or her authority to act for the individual.

The most common uses of a personal representative are:

- Parent acting on behalf of minor child;
- Guardian acting on behalf of incapacitated adult; and
- Family member acting on behalf of deceased person.

Employee wants help with his claim? OK, but get his signed HIPAA Authorization first.

For a sample HIPAA Authorization, see Sample Materials in this Guide.

Breaches

The Rules were expanded several years ago in order to hold health plans and business associates more accountable for maintaining the security of electronic PHI. Information must be kept secure, using administrative, physical, and technological safeguards, and breaches must be investigated.

Further, in the event of a breach or potential breach, the Plan is required to notify all affected individuals and the government. This is called a breach notification. If 500 or more individuals are affected in a single state, the media also must be informed.

What is a breach?

Breach means the unauthorized acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by the Rules and which compromises the security or privacy of the information.

The majority of breaches result from the loss or theft of computers, flash drives, or mobile devices with unencrypted data. If the data is encrypted, there is no breach. Encrypt!

Unsecured PHI means PHI that is not secured through the use of technology or methodology that makes PHI unusable, unreadable, or indecipherable to unauthorized persons. PHI is secured if:

- It is encrypted consistent with the National Institute of Standards and Technology (NIST) requirements; or
- It is completely destroyed (for example, hard copies are shredded and electronic media is destroyed using NIST guidelines).

What is a breach investigation?

As soon as a breach or potential breach is discovered, the Plan must investigate it and determine whether the PHI was secure (encrypted or properly destroyed). If secured, there is no breach and no further action is needed.

Next, even if not secured, the following three situations are deemed to not be breaches:

- Person receiving the PHI would not reasonably have been able to retain it;
- Acquisition, access, or use of PHI by employees or others acting under the authority of the Plan or a business associate was unintentional; or
- There were certain inadvertent disclosures among people similarly authorized to access PHI at the Plan or a business associate.

If none of the above applies, the Plan's investigation continues by performing a risk assessment. If the assessment determines that there is a low probability that the PHI was compromised, breach notifications are not needed. The risk assessment must, at a minimum, take into account:

- Nature and extent of PHI involved, including the types of identifiers and likelihood of re-identification;
- Identity of unauthorized person(s) who used or received the PHI;
- Whether the PHI was actually acquired or viewed; and
- Extent to which the risk to the PHI has been mitigated.

Inadvertent disclosures of PHI may happen from time to time, but not all disclosures are breaches.

If the incident meets any one of above exclusions, it is not a breach. In that case, the Plan documents the incident but the breach notification requirement is not triggered.

What is a breach notification?

In the event of a breach or potential breach (unless qualifying for an exception above), the Plan must notify HHS. If 500 or more individuals are affected by the breach, the Plan must submit an online report to HHS immediately (and if 500 or more are affected in a single state or jurisdiction, the local media also must be informed). For breaches affecting fewer than 500 individuals, the Plan will submit an online report to HHS in the year following discovery. For details, see HHS Portal to Report Breach of Unsecured PHI.

Regardless of the total number of individuals affected, the Plan must notify each affected person within 60 days of discovery. The notice must include:

- Brief description of what happened, including date of breach and date the breach was discovered;
- General description of the types of PHI (such as birthdates, Social Security or account numbers) but not the actual PHI;
- Information about the Plan's actions to mitigate the harm or prevent other breaches; and
- Description of steps the individual can take to protect against potential harm.

For a sample breach notification to individuals, see Sample Materials in this guide.

Penalties

HHS through its Office for Civil Rights (OCR) regulates and enforces the Rules. HHS can take direct enforcement action and assess civil monetary penalties against health plan sponsors (insurers and employers) and business associates (third-party administrators, brokers, etc.) for violations.

The current civil penalty amounts are:

- $112 per violation if the person does not know about the violation;
- $1,118 per violation due to reasonable cause;
- $11,182 per violation due to willful neglect that is corrected (generally within 30 days); and
- $55,910 per violation due to willful neglect that is not corrected.

Penalties are subject to an annual cap of $1,677,299 for violations of the same type. The amounts may be adjusted annually for inflation.

Reasonable cause means circumstances that would make it unreasonable, despite the exercise of ordinary business care and prudence, to comply with the provision violated.

Willful neglect means a conscious and intentional failure to comply or a reckless indifference to the obligation to comply.

To determine penalties in a particular case, HHS will investigate the facts and consider a number of mitigating and aggravating factors such as how many individuals were affected, how long the violation continued, and the extent of any harm. HHS also has discretion to resolve matters through corrective action with or without assessing a penalty.

The above are civil penalties. Criminal penalties, including imprisonment, also are possible although such cases usually involve intentional acts to obtain PHI under false pretenses or for personal gain.

Employer Checklist

Employers that sponsor group health plans are responsible for their plan's compliance with the Rules. Depending on the plan type and whether the employer has access to PHI, the employer's responsibilities may include some or all of the following:

- Identify all health plans (for example, medical, dental, vision, health flexible spending account (HFSA), health reimbursement arrangement (HRA), prescription drug).
- Determine the plan's funding method (either insured or self-funded).
- Determine whether employer will create, maintain, receive, or transmit PHI.
- Determine the plan's workforce (employees or job titles that will have access to PHI).
- Create firewall document (non-workforce employees cannot access PHI).
- Identify all business associates with access to PHI. Obtain business associate agreements.
- Designate a Privacy Officer. (Optional: Designate a Privacy Contact for routine matters.)
- Designate a Security Officer.
- Establish policies and procedures for:
  - Uses and disclosures
  - Individual rights
  - Administrative safeguards
  - Handling complaints
- Amend plan document to state that plan uses PHI (including electronic PHI) for plan administrative purposes and that procedures are in place to protect it.
- Create Notice of Privacy Practices (and reminder notice) and implement a distribution process.
- Create HIPAA Authorization forms and establish process for receiving and handling them.
- Identify all locations where PHI is maintained in hard copy or electronically.
- Develop a security policy explaining how electronic PHI is managed and protected.
- Review and address all standards required by Security Rule. Perform risk analysis.
- Create a breach investigation and breach notification process.
- Establish physical safeguards for locations or workstations where PHI is used or stored.
- Conduct workforce training, including new hires as needed, and document it.

Lastly, on periodic basis, review policies and procedures, perform risk analyses (for electronic PHI), and ensure documentation is maintained and up to date.

The Rules are complex and employers are encouraged to work with legal counsel to consider how the requirements apply to each employer's unique situation. Extensive federal guidance is provided at https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

Sample materials

The U.S. Department of Health and Human Services (HHS), through its Office for Civil Rights (OCR), regulates and enforces the Privacy Rule and Security Rule (Rules). The Department provides guidance to covered entities, including employers in their role as group health plan sponsors, to assist them in complying with the Rules. Based on the HHS guidance, ThinkHR has developed samples of some of the most common materials for employer-sponsored health plans:

- Notice of Privacy Practices
- Reminder of Availability of Notice of Privacy Practices
- Business Associate Agreement (BAA)
- Authorization Form
- Breach Notification to Individuals

Employers and their advisors are cautioned that sample materials cannot be used without careful review and customization for their group health plan's procedures and requirements. The samples are provided for the most common items and do not include all the materials that the employer may need. Employers are encouraged to work with legal counsel offering expertise in the Rules.

Sample

[*Words or phrases contained in brackets are intended as either optional language or as instructions to the user.*]

Notice of Privacy Practices

THIS NOTICE OF PRIVACY PRACTICES DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

[Insert name of group health plan(s)] (the "Plan") provides health benefits to eligible employees of [insert employer's name] ("we"), and their eligible dependents. The Plan creates, receives, uses, maintains, and discloses health information about Plan participants ("you"). The Plan has adopted policies to safeguard the privacy of your health information and comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This Notice is effective [insert effective date] and remains in effect until we change or replace it.

This Notice describes how your protected health information (PHI) may be used or disclosed to carry out treatment, payment, or healthcare operations, or for any other purposes that are permitted or required by law. It also describes the Plan's responsibilities and your rights with respect to your PHI.

Generally, PHI is health information, including demographic information, collected from you or created or received by a healthcare provider, a healthcare clearinghouse, a health plan, or your employer on behalf of a group health plan, from which it is possible to individually identify you and that relates to:

- your past, present, or future physical or mental health or condition;
- the provision of healthcare to you; or
- the past, present, or future payment for the provision of healthcare to you.

The Plan's Responsibilities

The Plan is required by law to:

- Ensure that health information that identifies you is kept private, except as such information is required or permitted to be disclosed by law;
- Describe the Plan's responsibilities and privacy practices with respect to your PHI;
- Abide by the terms of this Notice as currently in effect; and
- Inform you in the event of a breach of your unsecured PHI.

[*If you are covered by an insured health option under the Plan, you will also receive a separate notice from the insurance company or HMO.*]

How the Plan May Use and Disclose Your Information

The Plan and its business associates, which are service providers that assist us in administering the Plan or providing Plan services to you, use and disclose PHI in the ways described below. For purposes of this Notice, "the Plan" includes its business associates. We will not use or share your information other than as described in this Notice.

In order to administer your Plan coverage effectively, the Plan is permitted by law to use and disclose your PHI in certain ways without your authorization. The following list describes the ways that the Plan is legally allowed or required to use and disclose your PHI without your prior written authorization:

- **For treatment.** To ensure that you receive appropriate treatment and care, the Plan may use and disclose your PHI to coordinate care between the Plan and your provider. For example, we may disclose your PHI to healthcare providers for their treatment activities.

- **For payment.** To ensure that claims are paid accurately and you receive the correct benefits, the Plan may use and disclose your PHI to determine plan eligibility and responsibility for coverage and benefits. For example, the Plan may use and disclose your PHI when it confers with other health plans to resolve a coordination of benefits issue. The Plan may also use your PHI for utilization review activities.
- **For healthcare operations.** To ensure quality and efficient plan operations, the Plan may use and disclose your PHI in several ways, including plan administration, quality assessment and improvement, vendor review and for health care fraud and abuse detection and compliance. [Insert examples of how the Plan uses PHI for its operations, such as: For example, the Plan may use and disclose your PHI to assist in the evaluation of a vendor who supports the Plan for underwriting and related purposes. Another example includes the disclosure of your PHI to vendors to support our wellness initiatives.] The Plan is not allowed to use genetic information to decide whether to give you coverage or the price of that coverage.
- **Disclosures to the plan sponsor.** For the purpose of administration, the Plan may disclose PHI to certain employees of the Plan Sponsor ([insert employer name]). However, those employees will only use or disclose that information as necessary to perform plan administration functions or as otherwise required by HIPAA, unless you have authorized further disclosures. Your PHI cannot be used for employment purposes without your specific authorization.

Other Permitted Uses and Disclosures

Federal regulations allow us to use and disclose your PHI, without your authorization, for several additional purposes, in accordance with federal and state law:

- To a coroner or medical examiner;
- To cadaveric organ, eye or tissue donation programs;
- For research purposes, as long as certain privacy-related standards are satisfied;
  - Public health;
  - Reporting and notification of abuse, neglect or domestic violence;
  - Oversight activities of a health oversight agency;
  - Judicial and administrative proceedings;
  - Law enforcement;
  - To avert a serious threat to health or safety;
  - Specialized government functions (for example, military and veterans' activities, national security and intelligence, federal protective services, medical suitability determinations, correctional institutions and other law enforcement custodial situations);
  - Workers' compensation or similar programs established by law that provide benefits for work-related injuries or illness; and
  - Other purposes required by law, provided that the use or disclosure is limited to the relevant requirements of such law.

Also, for health and safety, and when consistent with applicable law and standards of ethical conduct, the Plan may disclose your PHI if the Plan, in good faith, believes that such disclosure is necessary to prevent or lessen a serious and imminent threat to your health or the health and safety of others.

Uses and Disclosures that You May Authorize

The following uses and disclosures will only be made with your written authorization:

- Uses and disclosures for marketing purposes;
- Uses and disclosures that constitute a sale of PHI;
- Most uses and disclosures of psychotherapy notes; and
- Other uses and disclosures not otherwise described in this Notice.

You may revoke your authorization in writing at any time by contacting us. (See "How to Contact Us" below.) Once we receive your written revocation, it will only be effective for future uses and disclosures. It will not be effective for any information that may have been used or disclosed in reliance upon your written authorization and prior to receiving your revocation. We also may continue to use and disclose your PHI after revocation if the authorization was obtained as a condition of securing insurance and other law provides us with the right to contest a claim under the policy or the policy itself.

Finally, if applicable state law provides you greater rights or protections concerning your PHI, we will follow such laws.

Your Rights

You have certain rights regarding access to, and the use and disclosure of your PHI as described below. To exercise any of these rights, contact us. (See "How to Contact Us" below.) Specifically, you have the right to:

- **Inspect and copy.** You have the right to inspect your PHI. Any request for access to your health information should be sent to us in writing. (See "How to Contact Us" below.) If the information you request is maintained electronically, and you request an electronic copy, we will provide a copy in the electronic form and format you request if the information can be readily produced in that form and format. If the information cannot be readily produced in that form and format, we will work with you to come to an agreement on form and format. We may deny your request in writing in certain, very limited circumstances. We may charge a reasonable, cost-based fee. If you are denied access, you may request that the denial be reviewed by submitting a written request to us.
- **Amend.** You have the right to request to amend your PHI if you think it is incorrect or incomplete. You must provide the request and your reason(s) for the request in writing to us. (See "How to Contact Us" below.) You will be notified in writing if your request is denied. If your request is denied, you have the right to submit a written statement disagreeing with the denial, which will be appended or linked to the health information in question.
- **Receive an accounting of disclosures.** You have the right to request a list of certain disclosures of your PHI that the Plan or our business associates have made. We will include all of the disclosures except for those about treatment, payment, health care operations and certain other disclosures (such as any you have asked us to make). Your request must be made in writing and state the time period of the request, which may not be longer than six years prior to your request. The first request within a 12-month period will be provided to you free of charge, and any additional requests within this time period may be subject to a reasonable, cost-based fee. The Plan will notify you prior to charging a fee, and you may choose to withdraw or modify your request at that time before any costs are incurred.
- **Be notified of a breach.** You have the right to be notified in the event that the Plan (or a business associate) discovers a breach of unsecured PHI.
- **Personal representatives.** You may exercise your rights through a personal representative. Your personal representative will be required to produce evidence of his or her authority to act on your behalf before that person will be given access to your PHI or allowed to take any action for you. The Plan retains discretion to deny a personal representative access to your PHI to the extent permissible under applicable law.
- **Obtain a copy of this Notice.** You have a right to receive a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time, even if you have previously agreed to receive the Notice electronically.

Complaints

If you believe that your privacy rights have been violated, you may file a complaint with the Plan or with the Office for Civil Rights of the U.S. Department of Health and Human Services. To file a complaint with the Plan, see "How to Contact Us" below. All complaints must be submitted in writing.

You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with the Plan.

How to Contact Us

The Plan has designated [insert name or title of Privacy Contact] as its contact person for all issues regarding the Plan's privacy practices and your privacy rights at [insert employer name, address, telephone number].

Sample

[*Words or phrases contained in brackets are intended as either optional language or as instructions to the user.*]

Reminder of Availability of Notice of Privacy Practices

The Privacy Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the [insert name of group health plan(s)] (the "Plan") to periodically send a reminder to participants about the availability of the Plan's Notice of Privacy Practices ("Privacy Notice") and how to obtain that notice. The Privacy Notice explains participants' rights and the Plan's legal duties with respect to protected health information (PHI) and how the Plan may use and disclose PHI.

To obtain a copy of the Privacy Notice, contact [insert employer name, address, telephone number], Attn: Privacy Contact. [You may also view the Privacy Notice online at [insert website address].]

You may also contact the Privacy Contact at [insert employer name, address] or call [insert telephone number] for more information on the Plan's privacy policies or your rights under HIPAA.

Sample

[*Words or phrases contained in brackets are intended as either optional language or as instructions to the user.*]

Business Associate Agreement (BAA)

Definitions

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

(a) **Business Associate.** "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) **Covered Entity.** "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Group Health Plan].

(c) **HIPAA Rules.** "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;
[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;
[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the 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;
[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;
[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the 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); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information
[Option 1 – Provide a specific list of permissible purposes.]
[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]
[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information
[Option 1] consistent with covered entity's minimum necessary policies and procedures.
[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the 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.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) **Term.** The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) **Termination for Cause.** Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) **Obligations of Business Associate Upon Termination.**
[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement.]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information 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.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) **Survival.** The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

Group Health Plan (Covered Entity):		**Business Associate:**	
By:	_____	By:	_____
Print Name:	_____	Print Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Sample

Authorization to Disclose Protected Health Information (PHI)
In accordance with the Health Insurance Portability and Accountability Act (HIPAA)

I hereby authorize the Plan:

To disclose _____

(description of health information to be disclosed (such as insurance claim information, treatment information))

to _____

(name or title of person or entity to receive information (name of health care provider, for example))

for the purpose of _____

(description of all purposes for the disclosure (for example, to recover overpayment from health care provider))

I understand that I may refuse to provide this authorization and that my eligibility for Plan benefits, or ability to obtain treatment or payment, will not be affected by my refusal.

I understand that I may revoke this authorization at any time in writing by sending a written request to the Plan's Privacy Contact. Revoking this authorization, however, will not have any effect on the Plan's use or disclosure of my Protected Health Information (PHI) before the Plan received the revocation.

I understand that if Protected Health Information (PHI) about me is disclosed to a person or organization that is not required to comply with federal privacy regulations, the information may be re-disclosed and no longer protected by the federal privacy regulations.

This authorization expires upon _____
(date or event)

_____ _____
Signature of Plan Participant (or Representative) Date

_____ _____
Print Name of Plan Participant Print Name of Representative *(if applicable)*

_____
Relationship of Representative to Plan Participant *(if applicable)*

[Name of Group Health Plan]

[ATTN: Privacy Contact]

[mailing address and telephone number]

Sample

[*Words or phrases contained in brackets are intended as either optional language or as instructions to the user.*]

Breach Notification to Individual

[Date]

[Name]

[Address]

Subject: Breach of Unsecured Protected Health Information

Dear :

On behalf of the [insert name of group health plan(s)] ("the Plan"), we are notifying you of a breach or potential breach of your Protected Health Information (PHI). PHI is individually identifiable health information that is created, received, stored, or transmitted by a covered entity (such as the Plan) and relates to the past, present, or future physical or mental health of the individual or information relating to the provision of care or payment for that care.

To the best of our knowledge:

- The breach occurred on or about _____. It was discovered on _____
- The information that may have been disclosed improperly includes _____

_____

We are investigating the circumstances surrounding this breach or potential breach. [Describe the investigative steps being taken and actions being put in place to protect against future breaches and to mitigate harm, and suggest actions the individual can consider to help protect him/herself.]

We are working diligently to correct the situation and mitigate any potential harm.

If you have any questions regarding this notice or the Plan's privacy practices, please contact:

[Name of Group Health Plan]

[Name of Plan Sponsor (Employer)]

ATTN: Privacy Contact

[Address and Telephone Number]