HIPAA Privacy and Security: Common Questions

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a broad federal law regarding health coverage. It contains provisions related to the portability of health coverage and provisions prohibiting discrimination by a health plan based upon an individual's health status. HIPAA also includes provisions relating to the privacy and security of personal health information.

- The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other protected health information (or PHI).
- The HIPAA Security Rule establishes national standards for securing individuals' electronic PHI (ePHI).

This Compliance Overview includes a set of common questions regarding the HIPAA Privacy and Security Rules.

LINKS AND RESOURCES

The U.S. Department of Health and Human Services (HHS) oversees HIPAA's Privacy and Security Rules. Click on the following links for more information:

- The HIPAA Privacy Rule
- The HIPAA Security Rule
- Information on compliance and enforcement

Affected Entities

Who is subject to the HIPAA Privacy and Security Rules?

The HIPAA Privacy and Security Rules directly apply to covered entities. Covered entities include:

- Health plans;
- Health care clearinghouses; and
- Health care providers that conduct certain transactions electronically.

The HIPAA Privacy and Security Rules indirectly regulate health plan sponsors. The extent of an employer's obligations under the HIPAA Privacy and Security Rules generally depends on whether the employer has access to PHI for plan administration purposes.

Other third parties that use PHI to provide services to covered entities (known as business associates) must also comply with certain provisions of the Privacy and Security Rules.

What is a "health plan?"

The HIPAA Privacy and Security Rules broadly define a "health plan" to include an individual or group plan that provides, or pays the cost of, medical care. This definition includes, for example, a group health plan (self-funded or fully insured), a health insurance issuer, a health maintenance organization (HMO) and an employee welfare arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

Self-administered, self-funded group health plans with fewer than 50 participants are not required to comply with the HIPAA Privacy and Security Rules.

The following benefits are NOT subject to the HIPAA Privacy and Security Rules:

- Accident only
- Disability income
- Life insurance
- Liability insurance
- Workers' compensation

Note: The benefits excluded under the HIPAA Privacy and Security Rules differ from those excluded under HIPAA's portability and nondiscrimination rules (for example, limited scope dental and vision plans ARE subject to the HIPAA Privacy and Security Rule).

What is a business associate?

The HIPAA Privacy Rule allows a covered entity to share PHI with a business associate. In general, a business associate means, with respect to a covered entity, 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.

The HIPAA Privacy Rule requires that a covered entity receive satisfactory assurances from the business associate in the form of a written contract.

The business associate standards do not apply to use and disclosure of PHI by a covered entity to a health care provider for treatment purposes or to the plan sponsor.

Does the HIPAA Privacy Rule apply to workplace wellness programs?

Since the HIPAA Privacy Rule applies only to covered entities and business associates (and not to employers in their capacity as employers-the application of the Privacy Rule to workplace wellness programs depends on the way in which those programs are structured. Some employers may offer a workplace wellness program as part of a group health plan for employees. For example, some employers may offer certain incentives or rewards related to group health plan benefits, such as reductions in premiums or cost-sharing amounts, in exchange for participation in a wellness program. Other employers may offer workplace wellness programs directly and not in connection with a group health plan.

Protected Health Information

What is protected health information (PHI)?

PHI is oral, written or electronic individually identifiable health information that:

- Is created or received by a covered entity; and
- Relates to 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.

The Privacy Rule applies to all types of PHI (written, oral and electronic). The Security Rule's requirements, however, only apply to electronic PHI (ePHI).

PHI does not include employment records held by a covered entity in its role as an employer.

What is de-identified information?

De-identified information is not governed by the HIPAA Privacy and Security Rules. The HIPAA Privacy Rule designates two methods that may be used to de-identify 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:

- Removes 18 specific identifiers; and
- Has no actual knowledge that the information could be used to identify the subject of the information (alone or in combination with other information).

What is summary health information?

In general, summary health information is health information that has most of its individual identifying information removed, but generally still qualifies as PHI. Summary health information may be disclosed to a plan sponsor for underwriting purposes or plan settlor functions (modifying, amending or terminating the plan), even without a plan amendment.

Summary health information is information that:

- May be individually identifiable;
- Summarizes claims history, claims expenses or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and
- Does not include the 18 identifiers required to be removed under the de-identification standards but may include five-digit zip codes.

Use and Disclosure Rules

When may a covered entity use and disclose PHI?

The HIPAA Privacy Rule allows covered entities to use and disclose PHI for treatment, payment or health care operations, subject to the minimum necessary standard.

In limited circumstances, the rules also allow covered entities to use and disclose PHI for purposes other than treatment, payment or health care operations, such as disclosures for workers' compensation, prevention of serious threat to health or safety, judicial or administrative proceedings and public health activities.

Also, a covered entity may allow a business associate to create, receive, maintain or transmit PHI on its behalf if a written business associate agreement is in place.

The HIPAA Privacy Rule requires an individual's authorization for uses and disclosures of PHI for purposes that are not otherwise permitted or required by law.

Treatment means the provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a patient, or the referral of a patient for health care from one health care provider to another.

Payment means the activities undertaken by a:

- Health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
- Health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Examples include determining eligibility for coverage, subrogation, billing, risk adjusting based upon enrollee health status and demographic characteristics, utilization review and review of medical necessity.

Health care operations means any of the following activities of a covered entity to the extent that the activities are compatible with and directly related to treatment or payment:

- Quality assessments and improvement activities;
- Population-based activities relating to improving health or reducing health care costs, case management and care coordination;
- Credentialing and health care provider evaluation;
- Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits (including stop-loss insurance and excess of loss insurance);

- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs; and
- Business planning and development, business management and general administration activities.

What is the minimum necessary standard?

In general, when a covered entity uses, discloses or request PHI, it must limit its use, disclosure or request to the **minimum necessary amount of information** to accomplish the intended purpose. Disclosures for treatment purposes and requests made by the patient for information regarding his or her own medical records are not subject to the minimum necessary standard.

Where a covered entity uses PHI, it must limit access to individuals (or classes of individuals) within its workforce that need access to carry out their duties. The covered entity is required to use reasonable safeguards (for example, locking filing cabinets that contain PHI and requiring the use of passwords to access electronic records containing PHI) to limit access to those individuals or classes of individuals that are deemed to need access. Where reasonable safeguards are present and the minimum necessary standard is applied, the HIPAA Privacy Rule permits certain incidental uses and disclosures that occur as a result of an otherwise permitted use or disclosure.

What provisions must be included within a business associate contract?

The HIPAA Privacy and Security Rules require that a covered entity receive satisfactory assurances from the business associate that it will appropriately handle and safeguard PHI. The business associate contract must establish the permitted and required uses and disclosures of PHI by the business associate. It must also require the business associate to:

- Implement appropriate safeguards (for example, limit access to employees on a need-to-know basis);
- 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 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.

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.

Also, a business associate that uses a subcontractor is required to enter into a business associate contract with the subcontractor.

Although a business associate contract is often required by HIPAA where a third party has access to PHI, provisions that are not required to be included should be reviewed carefully and are negotiable (for example, indemnification).

What is an authorization?

An authorization allows a covered entity to use and disclose PHI for purposes that are not otherwise permitted under the HIPAA Privacy Rule (that is, for purposes other than treatment, payment or health care operations).

What information must be included in a valid HIPAA authorization?

The following information must be contained—in plain language—in HIPAA authorizations:

- A description of the information to be used or disclosed, with sufficient specificity to allow the covered entity to know what information the authorization references;
- The name or other specific identification of the person/class of persons that are authorized to release the PHI;
- The name or other specific identification of the person/class of persons that are 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.

If the authorization is signed by a personal representative of the individual, the representative must indicate his or her authority to act for the individual. The individual should be provided with a copy of the signed authorization.

Does a plan sponsor need to obtain a signed authorization in order to assist an employee with a claim?

Yes. HIPAA requires that an insurance carrier or health care provider be provided with an authorization signed by the plan participant authorizing it to discuss PHI with a third party.

Can a plan sponsor get summary health information from the insurance carrier or TPA?

The HIPAA Privacy Rule permits a plan sponsor to receive summary health information for purposes of:

- Obtaining premium bids from health plans for the purpose of providing health insurance coverage (including securing stop loss coverage); and
- Modifying, amending or terminating the group health plans.

If a plan sponsor's access to medical information is limited to summary health information, it will not be required to comply with HIPAA's administrative requirements (for example, appointing a privacy officer, training employees, providing Privacy Notices or amending plan documents).

What does a plan sponsor need to do if it wants to get PHI from the insurance carrier or TPA?

HIPAA allows a plan sponsor to gain access to PHI for purposes of plan administration (for example, payment, quality assurance, claims processing, auditing, monitoring and management of carve-out plans) if:

- The group health plan amends its documents to allow the plan sponsor to have access to PHI for purposes of plan administration; and
- The plan sponsor certifies to the group health plan that the plan documents have been amended and that it agrees to the conditions described within the amendment.

HIPAA requires that a plan sponsor with access to PHI comply with all of the administrative requirements contained within the HIPAA Privacy and Security Rules. A plan sponsor's access to enrollment applications and disenrollment information ALONE does not qualify as having access to PHI for purposes of this requirement.

What about other federal and state laws regarding the privacy of health information?

The HIPAA Privacy Rule establishes a federal floor for privacy protections afforded to personal health information. States may pass laws which provide greater protections for medical records and other personal health information. However, the HIPAA Privacy Rule preempts any state law that is contrary to these federal regulations. In short, where federal and state law both govern medical privacy, the law that provides the individual with greater protection applies.

While the scope of the HIPAA Privacy Rule is quite large, it is also possible that some state laws may apply to entities that would not otherwise be required to comply with HIPAA's requirements. Employers should continue to be cognizant of other laws that govern privacy of health information, such as the Americans with Disabilities Act (ADA).

Security Safeguards

What steps do covered entities need to take to secure ePHI?

The HIPAA Security Rule requires covered entities to:

- Ensure the confidentiality, integrity and availability of all ePHI they create, receive, maintain or transmit;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of this information;
- Protect against reasonably anticipated uses or disclosures of this information that are 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.

According to HHS, **performing a risk analysis is a crucial first step** in identifying and implementing reasonable and appropriate security standards. It directs what reasonable steps a 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 standards are divided into three categories—**administrative safeguards, physical safeguards and technical safeguards**. Each type of safeguard has certain standards and implementation specifications associated with it. 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 to achieve the required security standards.

Covered entities are required to implement reasonable and appropriate policies and procedures to comply with the HIPAA Security Rule's standards and implementation specifications. A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of ePHI.

The Security Rule indirectly regulates employers as plan sponsors. 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 PHI will have fewer obligations under the Security Rule due to their "hands off" approach to PHI.

How should covered entities dispose of PHI?

Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI. For example, covered entities are not permitted to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons.

The Privacy and Security rules do not require a particular disposal method. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the form, type and amount of PHI to be disposed. For instance, the disposal of certain types of PHI (such as name, Social Security number, driver's license number, debit or credit card number, diagnosis, treatment information or other sensitive information) may warrant more care due to the risk that inappropriate access to this information may result in identity theft, employment or other discrimination, or harm to an individual's reputation.

In general, examples of proper disposal methods may include, but are not limited to:

- For PHI in paper records, shredding, burning, pulping or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable and otherwise cannot be reconstructed.
- Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
- For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains) or destroying the media (disintegration, pulverization, melting, incinerating or shredding).

Other methods of disposal also may be appropriate, depending on the circumstances. Covered entities are encouraged to consider the steps that other prudent health care and health information professionals are taking to protect patient privacy in connection with record disposal.

Administration

What are the administrative requirements of the HIPAA Privacy Rule?

In general, HIPAA requires a covered entity to do the following:

1. Limit its use and disclosure of PHI to activities related to treatment, payment and health care operations (unless specific patient authorization permits otherwise), including:
    - Limit access to PHI to employees on a need-to-know basis;
    - Establish procedures for routine disclosures that limit disclosure to the minimum necessary amount of PHI; and
    - For non-routine disclosures, develop reasonable criteria for determining and limiting disclosure to the minimum necessary amount of PHI.
2. Designate a privacy official who is responsible for the development and implementation of its privacy policies and procedures.
3. Train members of its workforce on its policies and procedures with respect to PHI.
4. Create written policies and procedures designed to ensure it complies with the HIPAA Privacy Rule.
5. Provide a process for individuals to make complaints concerning its policies and procedures related to use and disclosure of PHI.
6. Refrain from taking retaliatory action against an individual who makes a complaint—either with the covered entity or HHS—alleging a violation of the HIPAA Privacy Rule.
7. Establish and apply appropriate sanctions against business associates and members of its workforce that fail to comply with its privacy policies and procedures.
8. Mitigate, to the extent possible, the harmful effect of any violation of its privacy policies and procedures.
9. Not require individuals to waive their privacy rights as a condition of enrollment in the plan, eligibility for benefits, treatment or payment.

Exception for fully insured health plans: Group health plans that provide benefits solely through an insurance contract and do not create or receive PHI except for summary health information and/or enrollment information are only required to comply with Items 6 and 9 above.

Under the HIPAA Privacy Rule, do plan sponsors need to provide Privacy Notices?

A plan sponsor is required to provide employees covered under its group health plan with a Privacy Notice as follows:

- Where the plan sponsor is offering a fully insured group health plan and has access to PHI for plan administrative functions, it is required to provide a Privacy Notice upon request.
- If the plan sponsor is offering a self-funded group health plan, it must provide:
  - A Privacy Notice to all new enrollees
- at the time of enrollment;
  - A Privacy Notice within 60 days of a material revision to the notice; and
  - A statement that a Privacy Notice is available and how they may obtain a copy no less than every three years.

Where a plan sponsor is offering a fully insured group health plan and does not have access to PHI, it is not required to maintain or provide a Privacy Notice. A plan sponsor's access to enrollment applications and disenrollment information ALONE does not qualify as having access to PHI for purposes of this requirement. However, HIPAA requires that the insurance carrier provide a Privacy Notice.

*While the regulations require that the notices be provided to all "enrollees," a discussion within the preamble explains that providing the notice to the "named insured" or "employee" is acceptable.

Does the HIPAA Privacy Rule require a plan sponsor to amend its plan documents?

Where a plan sponsor has access to PHI, it is required to amend its plan documents. The plan amendment must:

- Establish the permitted uses and required disclosures of PHI;
- Describe the plan sponsor's employees or classes of employees that have been given access to PHI to conduct plan administration functions on behalf of the group health plan; and
- Provide an effective mechanism for resolving any issues of noncompliance by employees provided access to PHI.

A plan sponsor's access to enrollment applications and disenrollment information ALONE does not qualify as having access to PHI for purposes of this requirement.

Individual Rights

What are an individual's rights under the HIPAA Privacy Rule?

The rights provided to an individual under HIPAA include:

- A right to inspect or obtain a copy of his or her PHI;
- A right to request amendments or corrections to his or her PHI;
- A right to obtain an accounting of certain disclosures made of his or her PHI;
- A right to receive a privacy notice;
- A right to request restrictions on the use and disclosure of his or her PHI;
- A right to request confidential communications of his or her PHI; and
- A right to challenge use of his or her own PHI through the complaint processes established by a) the covered entity and b) the Secretary of HHS.

Can individuals sue if their privacy rights are violated?

The HIPAA Privacy and Security Rules do not provide a private right to sue. HHS' Office of Civil Rights (OCR) has the authority to accept and investigate complaints and conduct compliance reviews. The HIPAA Privacy and Security Rules include both civil and criminal sanctions for failure to comply. While the HIPAA Privacy and Security Rule does not directly provide a private right to sue, an individual may have other legal remedies, including:

- ERISA remedies where a plan has failed to follow provisions within its plan documents;
- Breach of contract remedies;
- Violation of state privacy laws; and
- Professional sanctions (for example, accountants, attorneys and physicians).
