



HIPAA Privacy, Security & HITECH Frequently Asked Questions (FAQs)

Table of Contents

- [Overview](#) Page 1
- [Covered Entity](#) Page 2
- [Protected Health Information \(PHI\) & Health Information](#)... Pages 2-3
- [HIPAA Regulated & Non-Regulated Benefits](#) Page 4
- [Violations & Breaches](#)..... Pages 4-5
- [Enforcement & Safeguards](#)..... Pages 5-6
- [Training Requirement](#)..... Page 6

Overview

(1) What is HIPAA?

The Health Insurance Portability & Accountability Act (HIPAA), enacted by Congress in 1996, established national regulations for the use and disclosure of an individual's health information. Essentially, a Privacy Rule was created to define how covered entities use individually identifiable health information or Personal Health Information (PHI) by requiring covered entities to implement reasonable policies and procedures to keep PHI confidential. A Security Rule was established to ensure the confidentiality, integrity and availability of electronic PHI (ePHI).

(2) What is Health Information Technology for Economic and Clinical Health Act (HITECH)?

HITECH, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information.

Covered Entity

(3) Is the State of Delaware considered a covered entity?

Yes. The State of Delaware's Group Health Insurance Program ("The Plan") is a covered entity. Individuals, organizations and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

Protected Health Information (PHI) & Health Information

(4) What is Protected Health Information (PHI)?

PHI, includes individually identifiable health information that either identifies an individual or with a reasonable basis to believe that an individual can be identified using information that is transmitted or maintained by a covered entity in any form or media, including electronic, oral and written. The privacy rule lists 18 ways an individual can be identified, including name, social security number, member identification number, email and postal addresses, phone number, license number, picture, etc. Having just one of these identifiers is enough to make the data individually identifiable!

(5) What is Health Information?

Health information means any information, including genetic information, whether oral or recorded in any form that:

- a. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse (health care clearinghouses process healthcare transactions on behalf of providers and plans); and
- b. Relates to the past, present or future physical or mental health or condition of an individual; the provisions of health care to an individual; or the past, present or future payment for the provision of health care to an individual.

(6) What types of PHI could you handle?

Examples of types of PHI you could handle include:

- Eligibility information
- Enrollment information
- Claims information
- Claims appeals
- Coordination of Benefits (COB) determinations
- Medical condition information

(7) Can PHI be used by the State of Delaware for discipline, hiring, terminating employment, promotions and/or demotions?

No. PHI will *NOT* be used by the State of Delaware for discipline, hiring, terminating employment, promotions and/or demotions.

(8) How can PHI be used and disclosed?

Unless allowed by the Privacy Rule, the Group Health Plan (technically, the staff that administer these plans) are required to protect PHI and *ONLY* use or disclose/release PHI for the following reasons:

- To the individual – about the individual.
- For treatment, payment and health care operations.
- For legally permissible reasons (such as , for public health reasons, in response to a court order or subpoena, to a coroner, medical examiner or funeral director, etc.).
- With a signed HIPAA authorization form from the individual.
- To the federal and/or state Department of Health and Human Services for enforcement reason(s).

Human Resources staff can discuss general coverage and eligibility rules with participants' family members – NOT PHI. PHI may not be discussed with anyone outside of the covered entity except the individual (not even the spouse) without a signed authorization, unless the individual is present and the individual is given an opportunity to object and does not. The other exception is in the case of an emergency where the individual is incapacitated.

As a covered entity, the State of Delaware may also release PHI *without* an authorization for certain reasons such as:

- For public health reasons (i.e., disease outbreaks, etc.).
- Individual may be the victim of abuse, neglect or domestic violence.
- In response to a court order or subpoena.
- To the coroner or medical examiner.
- To avert a serious threat to health or safety.
- To comply with Workers' Compensation laws.

(9) What is the HIPAA Security Rule?

The Security Rule only covers electronic PHI (ePHI) that is maintained or transmitted electronically. Examples include PHI sent/received via email, PHI stored in computers, networks and servers and PHI stored on portable electronic media (CDs, disks and tapes). The Security Rule protects against any reasonably anticipated threats to the security or integrity of ePHI.

HIPAA Regulated & Non-Regulated Benefits

(10) What benefits does HIPAA regulate?

Benefit programs sponsored by the State of Delaware that are HIPAA regulated include:

- Group Health Plans
- Dental plans
- Vision plans
- Claims Administrators
- Pharmacy benefit managers (PBMs)
- Flexible Spending Accounts (FSAs)
- Health Reimbursement Arrangements (HRAs)
- Consolidated Omnibus Budget Reconciliation Act (COBRA)

(11) What benefits are *not* HIPAA regulated?

Although this information is confidential, HIPAA does not cover:

- Life and Accidental Death & Dismemberment insurance
- Workers' Compensation
- Short Term Disability
- Long Term Disability
- Pension plans

(12) Are employment records HIPAA regulated?

No. Although employment records held by the State of Delaware as an employer are confidential, they are *not* subject to HIPAA. Examples of employment records include:

- FMLA requests
- Americans with Disabilities (ADA) records
- Workers' Compensation records
- OSHA reports
- Disability records
- Sick leave requests or justifications
- Return-to-Work data
- Drug screening results/alcohol and drug free workplace data
- Fitness for duty exams

Violations & Breaches

(13) What are the penalties for HIPAA violations?

There is a tiered penalty structure for violations based on the intent behind the violation and can reach up to \$1.5 million per year per standard or higher. Penalties are mandatory in situations involving "willful neglect" and a formal investigation is required.

Covered entities are liable for their employees' actions **and** employees may be subject to criminal charges.

(14) What does willful neglect mean?

"Willful neglect" essentially means "being clueless and/or cavalier". Here are some examples:

- You send an email containing PHI unsecurely.
- You have no demonstrable evidence that you are requiring HIPAA training as required by the HIPAA regulations.
- You have no plan to show how you are working on full HIPAA compliance, despite the fact that you are aware that you are not in full compliance at the moment.
- Your employees have their passwords on "sticky notes" that are readily visible.
- Employees are throwing away papers containing PHI rather than shredding them.

(15) What happens if a breach occurs?

Covered entities (including group health plans) must notify individuals when there is a breach of all forms of "unsecured PHI" for incidents occurring on or after September 23, 2009. HIPAA also requires notice be provided to the State and/or the Federal Department of Health & Human Services and the media on occasion.

Enforcement & Safeguards

(16) How can you protect PHI and enforce the HIPAA regulations?

- Do NOT share your password with anyone!
- Lock file cabinets that contain sensitive and confidential information.
- Think before you click "send."
- Use secure email (EGRESS Switch) when transmitting PHI.
- Keep it "quiet." Share PHI on a need to know basis only.
- Don't store PHI on laptops, but if you do, ensure the laptop is encrypted to avoid breaches.
- Don't access emails or documents containing PHI from mobile devices.
- Shred trash containing PHI instead of throwing it away.
- Ensure that electronic media containing PHI is erased/sanitized before reuse.

(17) What electronic safeguards are in place that impact your daily operations?

Your workstation security includes:

- Unique user IDs.
- Complex passwords that age at regular intervals.

- Sessions timing out due to inactivity.
- Account lockouts due to failed login attempts.
- Access to ePHI according to job class.
- Limited access to the internet.
- Limited access to laptops and portable devices.
- Limited access to remote connections.
- DTI monitoring of your activity online.

Training Requirement

(18) How can I learn more about HIPAA?

SBO offers two online HIPAA courses:

a. *HIPAA Privacy, Security and HITECH Training*

This online course, which takes approximately one hour to complete, provides employees with information on HIPAA and their responsibility for guarding Protected Health Information (PHI) and enforcing regulations. All human resources, benefits and payroll staff, as well as all other employees who have access to PHI, are **required** to complete this course every two years.

b. *HIPAA Privacy, Security and HITECH Training – For Supervisors and Managers*

This online course, which takes approximately 30 minutes to complete, is specifically designed and recommended for all supervisors and managers. Supervisors and managers may have access to documents and information containing individually identifiable health insurance for their employees, so it is important they are aware of HIPAA and their responsibility for guarding employees PHI and enforcing regulations. Supervisors and managers are **highly encouraged** to complete this course every two years. *Note: Supervisors and managers that work in human resources, benefits or payroll **must** complete the standard HIPAA Privacy, Security and HITECH Training mentioned in “a” above. If you complete the training mentioned in “a” above, you are not required to complete the “HIPAA Privacy, Security and HITECH Training – For Supervisors and Managers.”*

Access instructions, FAQs and both course links are located at www.ben.omb.delaware.gov/hipaa.