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

Table of Contents

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. The purpose of HIPAA can be outlined in three main topics: (1) The Privacy Rule sets standards for the protection of health information; (2) The Security Rule sets standards for protecting health information that is held or transferred in electronic form; and (3) The Breach Notification Rule establishes the actions to be taken in the event a breach occurs.

(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 (or GHIP) is considered a Covered Entity, meaning that the workforce of all organizations who participate in the GHIP are subject to HIPAA requirements. The State of Delaware is required by federal law to provide HIPAA training to all those covered under the organizations, whether State or participating groups, who are members of the HIPAA workforce, in other words, those who have access to PHI as a part of their job.

Protected Health Information (PHI) & Health Information

(4) What is Protected Health Information (PHI)?
Protected Health Information is information that relates to an individual's past, present, or future physical or mental health or condition, the provision of health care services or supplies to the individual, or payment for health care services or supplies to an individual that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual and is transferred or maintained by a Covered Entity in any form or medium (electronically, orally or written). Protected Health Information includes many common identifiers such as social security number, name, account number, member identification number, postal address, phone number, picture, and license number. Think of an identifier as information a stranger could use to relate health information to a specific person. Types of PHI someone might handle consist of information related to eligibility, enrollment, claims, claims appeals, reports from third-party administrators or other vendors, Explanation of Benefits (or EOBs), and medical providers' bills. If the PHI is maintained, stored or transmitted electronically, it is referred to as Electronic Protected Health Information (or ePHI).

(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?
Types of PHI someone might handle consist of information related to eligibility, enrollment, claims, claims appeals, reports from third-party administrators or other vendors, Explanation of Benefits (or EOBs), and medical providers' bills.

(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 ePHI that is maintained, stored or transmitted electronically. Examples include:

- PHI sent/received via email
- PHI stored in computers, networks and servers
- 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. There are three categories of safeguards that are specified under the rule – administrative, physical and technical. The administrative safeguards include risk analysis and management, training programs, handling of security incidents and sanctions, account access and management and disaster recovery planning. The physical safeguards include the development of a security plan for the location, limiting access to offices and professional spaces based on job needs, visitor controls, workstation use and security and disposal or re-use of hardware and media. The technical safeguards include system access controls, protection and monitoring, data integrity, audit controls and data encryption and decryption.

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 Plan
- Health Reimbursement Account
- Prescription Plan
- Dental Plan
- Employee Assistance Program
- Dela*WELL*
- Vision Plan
- Health Care Flexible Spending Account
- COBRA

(11) What benefits are *not* HIPAA regulated?
Although this information is confidential, HIPAA does not cover:

- Group Universal Life and Accidental Death & Dismemberment
- Workers' Compensation
- Short Term Disability
- Long Term Disability
- Dependent Care Flexible Spending Account
- Supplemental Benefits
- Deferred Compensation
- Pension Plan

(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?
The "Complaint Form Regarding Handing of Protected Health Information" is located on the SBO website under "HIPAA" and contains instructions for completion and submission. If a HIPAA breach is detected, the Statewide Benefits Office (SBO) needs to be notified immediately. SBO will then determine if notification is necessary and who

must be contacted. If notification is required, individuals will receive a letter within 60 days of the discovery of the HIPAA breach.

If you know or believe a HIPAA breach has occurred, notify SBO immediately.

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) Who is required to complete SBO's HIPAA Training for Members of the HIPAA Workforce Certification?
The State of Delaware's Group Health Insurance Program (GHIP) is considered a covered entity, meaning that the workforce of all organizations who participate in the GHIP are subject to Health Insurance Portability & Accountability Act (HIPAA) requirements. The State of Delaware is required by federal law to provide HIPAA training to all those covered under the organizations who are members of the HIPAA workforce, in other words, those who have access to Protected Health Information (PHI) as a part of their job. This training is intended to satisfy the U.S. Department of Health & Human Services

(HHS) requirement for HIPAA training and is designed specifically for members of the HIPAA workforce, including employees and individuals with access to HR, benefits and/or payroll data as part of their job-related tasks, as well as supervisors and managers. Employees and individuals who fall within these categories are **required** by the State of Delaware to complete the SBO online "HIPAA Training for Members of the HIPAA Workforce" Certification **every two years** to ensure they understand their role in the proper use and distribution of PHI.

Please note: *HIPAA training courses (online or in-person sponsored by organizations other than SBO will not satisfy this requirement). This training does not apply to employees or individuals without access to HR, benefits and/or payroll data as part of their job-related tasks. Any change to the federal HIPAA regulations and/or change in our HIPAA policies and procedures and/or the training course content may require an individual to complete an updated version of the online course prior to their two-year timeframe. They will receive notification if this occurs.*

Access the HIPAA Training at de.gov/statewidebenefits.