BARROW LENT LLP
BENEFITS | EMPLOYMENT | LITIGATION

HIPAA Privacy Overview

Alera Group

June 16, 2025

Stacy H. Barrow
sbarrow@marbarlaw.com
(617) 830-5457

Housekeeping Items

- All attendees are muted to ensure audio quality throughout the webinar.
- Use the Q&A box in your navigation bar to ask our speaker your questions. We will address as many live questions as possible during today's presentation.
- This webinar is being recorded and an on-demand recording will be shared with you.
- Thank you for joining!

Overview of Presentation

- HIPAA Core Concepts
- Uses and Disclosures of PHI
- Individual Rights of Participants
- Safeguards for Protecting PHI
- Breach Notification Requirement

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
  - Access to health care (e.g., portability, special enrollment, nondiscrimination)
  - "Administrative Simplification" rules (e.g., privacy, security, coding for health care transactions)
- The purpose of HIPAA's Administrative Simplification rules were to improve efficiency and effectiveness of the health care system by standardizing the electronic exchange of administrative and financial data

HIPAA Privacy Rule & Security Rule

- The HIPAA Privacy Rule and Security Rule protect individually identifiable health information
  - **Purpose of the Privacy Rule:** Sets rules for how a covered entity may use and disclose PHI and gives participants certain rights regarding the protection of and access to their PHI
  - **Purpose of the Security Rule:** Protects against reasonably anticipated threats of uses or disclosures of electronic PHI (e-PHI) that are not allowed by the Privacy Rule
    - Requires a covered entity to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI

What is the Covered Entity?

- The HIPAA Privacy rules apply (although sometimes in different ways) to all "covered entities":
    i. health plans;
    ii. health care clearinghouses; and
    iii. health care providers who transmit any health information in electronic form in connection with one of the transactions covered by HIPAA
- The rules also apply to a health plan's "Business Associates"
- Many organizations that have health information are not subject to HIPAA
  – Examples include employers, workers compensation carriers, many state agencies like child protective service agencies

Covered Entities: Health Plans

- What is a Health Plan under HIPAA?
  - Employer sponsored health plans are “health plans” under HIPAA (includes health FSAs)
    - Exception for plans that are self-insured, self-administered by the employer (no TPA), and that have less than 50 eligible participants
  - HMOs and health insurers are also health plans under HIPAA. Those fully-insured plans are responsible for HIPAA compliance and employers are also responsible – if they receive PHI
- What is NOT a health plan under HIPAA?
  - Pension and Disability insurers or benefits are **NOT** covered by HIPAA
  - Life, property or casualty insurers or benefits are **NOT** covered by HIPAA
  - Workers’ compensation insurers or benefits are **NOT** covered by HIPAA

What Type of Benefits Are Covered?

- Medical (physicians, hospitals)
- Vision
- Dental
- Hearing
- Behavioral Health
- Substance Use Disorder
- Prescription Drug Coverage

Consequences of Non-Compliance

- Significant civil, monetary and criminal penalties for failure to comply with HIPAA
  - Rules enforced, including civil monetary penalties, by the Office of Civil Rights, not the DOL or the IRS
  - Criminal action prosecuted by Department of Justice
- Potential litigation for breach of HIPAA rules
  - There is no private right of action under HIPAA
- Notification of breaches
- Employers may discipline any employee who violates HIPAA

Consequences of Non-Compliance

Violation Category	Per Violation Penalty	Annual Cap for All Violations of an Identical Provision
Did Not Know	$100 - $50,000	$25,000
Reasonable Cause	$1,000 - $50,000	$100,000
Willful Neglect-Corrected	$10,000 - $50,000	$250,000
Willful Neglect-Not Corrected	$50,000	$1,500,000

HIPAA Violations in the News

- **Lessons Learned from HIPAA Violations**
  - Don’t use unsupported software (i.e., out-of-date versions) and apply patches regularly and promptly
  - Train workforce that snooping is forbidden and a HIPAA violation
  - After routine IT maintenance, always check that firewalls are reactivated, and security settings are appropriate
  - Wipe any hard drives (which many copiers have) before reselling or returning to leasing companies
  - Implement strong policies and procedures regarding taking PHI offsite, handling while offsite and protecting it from others (family members, neighbors, visitors in the home, etc.)
  - Never leave PHI or a device containing PHI in a vehicle unless the PHI or device is secured
  - Review business associate agreements (and subcontractor BAAs) to make sure they’ve been updated for legal requirements and any changes in the services to be rendered by the business associate

Definition: Protected Health Information (PHI)

- The HIPAA Privacy Rules apply to Protected Health Information
- Protected Health Information (PHI) is **individually identifiable health information** in any form – paper, oral, electronic, that is created, maintained or received by a Covered Entity
- PHI excludes employment records held by an employer in its role as an employer (e.g., physician's note submitted by employee documenting reason for absence from office)
- Covered Entities must protect PHI of deceased individuals for at least 50 years

What is Health Information?

- Health information includes any information created by a health care provider, health plan, employer, school, or university that relates to:
  - the past, present, or future physical or mental health or condition of the individual;
  - the provision of health care to the individual; or
  - the past, present or future payment for health care to the individual

What Makes Health Information Individually Identifiable?

- Name
- Dates: birth, admission to hospital, discharge from hospital, death
- Telephone and fax numbers
- Social Security Number
- Account number
- Vehicle identifiers including license plates
- Web URLs and IP address numbers
- Genetic Information
- Geographic unit (certain zip code information excepted)
- Ages over 89
- E-mail and other addresses
- Medical record numbers and health plan numbers
- Certificate or license number
- Device identifiers and serial numbers
- Biometric identifiers, including finger and voice prints and full face and other identifying photographic images

Examples of PHI

- Information that is PHI:
  - Claims related information (e.g., EOBs, calls from employees to the plan, etc.)
  - Summaries of claims information from vendors that include identifiers
  - List of plan participants
- Information that is not PHI:
  - Doctor's note provided to manager (e.g., sick leave purposes)
  - Health information contained in FMLA or ADA requests
    - Employers must maintain all information about employee illness as a confidential medical record in compliance with the ADA
  - De-identified information (e.g., aggregate claims statistics)

What About Enrollment Information?

- Enrollment information (including premium contribution amounts) has special, dual status—it is not PHI in the hands of the employer, but it is PHI in the hands of the insurance carrier or covered entity
- Only authorized employees and business associates may have access to PHI and only for plan administration purposes

HIPAA Privacy: The Basic Rules

- An employer's health plan(s) may use and disclose PHI for **T**reatment, **P**ayment, and health care **O**perations of the plan ("TPO Purposes")
- Most other uses or disclosure of PHI require a signed, written authorization
- An employer's health plan(s) have to give certain rights to individuals
  - For example, right of access by a participant to his or her records, right to propose a change to the record, and accounting of disclosures
  - The handling of these rights can be delegated to the third-party administrators
- Administrative Requirements: Training, privacy officer, privacy notice, many policies, procedures and sanctions for violations

Typical Allowable Uses and Disclosures Without Any Written Permission

- Enrollment
  - use internally, or
  - disclose to the employer's health plan's vendors
- Eligibility
  - use internally, or
  - disclose to the employer's health plan's vendors, or
  - disclose to health care providers
- Claims adjudication and payment
- Pre-certification and referral
- Coordination of benefits
- Utilization review
- Review of status of claims payment
- Use of de-identified information

Examples of PHI Use That Require Authorization

- Authorization required when:
  - Disclosing PHI to an FMLA administrator so he/she can determine if an employee is eligible for FMLA leave
  - Giving a manager PHI about an employee's medical condition so he/she can make an ADA accommodation

Protections for Reproductive Healthcare Information

- Regulations released in April 2024 prohibit the use or disclosure of PHI to:
  - conduct a criminal, civil, or administrative investigation into or impose any such liability on any person for the act of seeking, obtaining, providing, or facilitating reproductive health care, or
  - identify any person for the purpose of investigating or imposing liability, when the Covered Entity reasonably determines that one or more of the following exists:
    - The reproductive health care is lawful where it was provided and under the circumstances;
    - The reproductive health care is protected, required, or authorized by Federal law, including the Constitution, regardless of the state in which such health care is provided; or
    - The reproductive health care is provided by a person other than the Covered Entity that receives the request for PHI and it is presumed to have been legally provided care

Protections for Reproductive Healthcare Information

- The regulations do not prohibit Covered Entities from using or disclosing PHI for purposes otherwise permitted under the Privacy Rule where the request for PHI is not made for purposes of investigating or imposing liability on any person for seeking, obtaining, providing, or facilitating reproductive health care
  - The HIPAA Workforce should understand how to identify and respond to any requests that may potentially relate to reproductive health care
- The new regulations were effective on June 25, 2024, and required compliance by December 23, 2024
- An updated Notice of Privacy Practices will need to be provided to participants by February 16, 2026
  - HHS intends to publish an updated model Notices of Privacy Practices

The Key Requirements

- Training
- Privacy Officer
- Privacy Notice
- Authorization
- Minimum Necessary
- Safeguards
- Participants’ Rights as Individuals
- Vendors - Business Associates
- Handling Complaints
- Employee Sanctions
- Policies & Procedures

Mandatory Training Under Privacy Rule: Why are We Listening to This?

- An employer's health plans must train all participants of its workforce with access to PHI ("HIPAA Workforce") regarding HIPAA privacy policies and procedures, as necessary and appropriate for the participants of the workforce to carry out their job duties
  - Each new participant of the workforce with access to PHI must be trained within a reasonable period of time after their hire date
- All training must be documented

Privacy Officer

- Under HIPAA, all health plans must have a privacy officer
- The privacy officer is responsible for developing and implementing policies and procedures necessary to comply with HIPAA privacy rules, including training
- Employers must also designate a contact person to answer questions and receive complaints about HIPAA's privacy rules, and to obtain the forms necessary for a participant to exercise any of his or her rights under HIPAA
- Fully insured plans that do not receive any PHI (other than Summary Health Information) have a limited HIPAA obligation
  - Among other things, such plans avoid the need to name a privacy officer, deliver a privacy notice (the carrier does it on behalf of fully insured plans), or maintain privacy policies and procedures (and train their employees on them)

Privacy Notice

- HIPAA requires covered entities to develop and distribute a notice that provides a clear, user friendly explanation of individuals rights with respect to their PHI and the plan's privacy practices
  - Notices can be delivered by e-mail, if a participant agrees to electronic notice
  - The privacy notice must be distributed upon enrollment to all new participants
  - An employer's intranet may include a copy of the privacy notice
  - Participants are entitled to paper copies upon request
  - An employer's health plans cannot substantially change their information policies and procedures before updating its notice to reflect those revisions
- At least once every 3 years, an employer's health plans must remind participants of the availability of the privacy notice

Authorizations

- Most disclosures of PHI require authorization
  - For example, if an employer wants to use the plan's own health plan records to see if a participant is entitled to disability benefits, participant must sign an authorization
  - Written authorization is not required if PHI is being used by the plan for treatment, payment or health care operations purposes (or for other disclosures permitted by the privacy rules)
- Employers should seek a written authorization from the individual before releasing the individual's PHI to most third parties
- Employers should seek authorization from individuals before using PHI for reasons other than payment or health care operations

Interaction with Participants and Family

- Individuals may ask for assistance with plan benefits
  - If (1) disclosure is to a family member involved in the individual's care or payment for that care, (2) disclosure is limited to that family member's involvement in the care or payment and (3) the individual has not objected to the disclosure to the family member, then it's okay to disclose, but preferable to refer to your outside administrators
  - With a complete authorization, or another legal document, such as a general power of attorney, an employer could disclose anything to the family member
  - Contact your ***Privacy Officer*** before disclosing PHI to anyone claiming to be a personal representative of a participant
    - ***Privacy Officer*** will confirm that the individual has met all legal requirements to be a personal representative

What Can I Discuss?

- Employees can always pass on information from a spouse to the plan or, if for purposes of payment or operations, to the plan's vendors
- You can discuss the medical claims of a child (under 18) with either parent (subject to limited exceptions - e.g., records protected under federal laws on family planning), unless the employer is notified that it is not appropriate to so share the information (e.g., domestic abuse)
- You may disclose PHI to family members of a deceased participant who were involved with the participant's care or payment for their care, so long as such disclosure is not contrary to any prior expressed preference of the individual that is known to the plan

“Minimum Necessary” Rule

- The “Minimum Necessary” Rule
  - Whenever the health plan uses or discloses PHI or requests PHI from another plan or a physician, it “must make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure or request”
  - Thus, the minimum necessary rule covers
    - HR Department’s use of information
    - Verbal disclosures
    - Requests for disclosure

“Minimum Necessary” Rule

- The minimum necessary rule does not apply to:
  - Disclosures to or requests by a health care provider for treatment
  - Disclosures to the individual or pursuant to an authorization
  - Disclosures to government for enforcement of privacy rules
  - Other uses or disclosures required by law
    - Special protections apply to reproductive healthcare information

“Minimum Necessary” Rule

- Only use PHI when it’s necessary to perform your job duties
- Use only the minimum necessary PHI to perform your job duties
- Follow your employer’s HIPAA policies and procedures for confidentiality and security
- Do not disclose PHI to other employees that are not authorized to receive it
- ***Ask*** if you have questions about what you can and can’t disclose

Limiting Employee Access to PHI

- Employers must identify those persons or classes of persons in its workforce who need access to PHI to carry out their duties ("HIPAA Workforce"):
  - Privacy Officer
  - Human Resources to the extent that they handle benefits issues related to the employer's group health plan
  - Members of the Information Technology department may also have access to PHI

Limiting Employee Access to PHI

- Only HIPAA Workforce may have electronic and physical access to PHI—all others should avoid seeing (or using) PHI
  - HIPAA Workforce may use and disclose the Plan's PHI only for plan administrative functions
  - The amount of PHI disclosed must be limited to the minimum amount necessary to perform the relevant plan administrative functions
  - Generally, HIPAA Workforce may not disclose PHI to employees other than other HIPAA Workforce

Safeguards to Protect Privacy

- PHI may not be filed in the same files as any other employee HR information, including personnel records, and electronic access must be restricted to only HIPAA Workforce
- HIPAA Workforce have their own computer passwords and user domain account passwords accessible only to HIPAA Workforce, and they may not share passwords
- Lock cabinets and doors to offices that contain health plan records
- Be cognizant of discussions—discuss PHI only in a "controlled environment"
- Take precautions—if you are in a position to hear, take precautions not to hear if you have no need to hear

Individual Rights

- Right to Inspect and Copy PHI in the plan's records
- Right to Propose an Amendment to Correct PHI in the health plan's records
- Right to remove non-paid claims from PHI data set
- Right to an Accounting of Disclosures
- Right to Request Restrictions on PHI Use & Disclosure
- Handling of these rights may have been delegated to vendors

Individual Rights

- Copying and proposing amendments
- Participants and dependents have the following rights under HIPAA:
- To access, inspect and copy their health information records in the health plan's records
- To copy any enrollment, payment, claims adjudication, and case or medical management records system that includes PHI and that is maintained by or for the health plans or used in whole or in part by the health plans to make decisions about individuals
- Right to propose an amendment to the PHI or a record about the participant (or dependent) in the health plan's record sets

Individual Rights

- Accounting of disclosures
- Participants have a right to request from the health plans an accounting of the disclosures of their PHI
- An employer must keep a log of disclosures of PHI made within 6 years prior to the request, and be able to give that log to a participant upon request
- An employer may require HIPAA Workforce to keep track of additional disclosures

Individual Rights

- Confidential Communications
- HIPAA grants adult dependents (e.g., spouse, adult children) the right to request that the plan send them communications (including any EOB that the plan may mail out) by alternative means or at alternate locations from the mailing address of the named insured
- Privacy notice advises participants of this right
- The health plans only needs to accommodate the request if the request is reasonable and the individual specifies that the disclosure of all or part of the health information would endanger the individual (e.g., domestic abuse)

Individual Rights

- If you are contacted by a participant who wants to exercise one of these rights, contact your Privacy Officer
- These are not absolute rights
- In most cases, the participant's request should be forwarded to the applicable insurance carrier or claims administrator
  - TPAs are generally required to respond to such requests per the client's Business Associate Agreements with them
- If an employee (or covered dependent) complains his or her health plan privacy rights have been violated, the person complaining should be directed to the Privacy Officer

What is a Business Associate?

- Definition:
- A person who (i) performs for or on behalf of a covered entity, or assists a covered entity, in performing an activity or function involving use or disclosure of health information (e.g., claims processing, utilization review, billing), or (ii) provides legal, actuarial, accounting, management, administrative, accreditation or financial services where the provision of such services involves the disclosure of health information from the entity or another business associate of the entity
- Includes anyone with health information from your health plans (could include attorneys, benefit brokers/consultants, TPAs, auditors, computer software service companies)

What are the Business Associate Rules?

- General Rules
  - Need specific HIPAA-dictated language in a contract with all business associates
  - Language includes privacy protections as well as the extension to service providers of individuals' HIPAA rights
  - So, when entering into a new agreement with a third-party administrator or a benefits consultant, the Privacy Officer must arrange to have this language in your agreement

What are the Business Associate Rules?

- Privacy and Security Requirements under HITECH Act (2009)
- Under HITECH, all of the HIPAA rules apply directly to business associates, including penalties
  - Previously, HIPAA applied only to “covered entities” – health plans, health care providers, and clearinghouses
  - HIPAA applied indirectly to business associates – through business associate agreements
  - Business associates, like brokers and consultants, perform PHI-related functions for group health plans

Handling Complaints

- The Privacy Notice advises everyone that they have a right to complain, about violations of their HIPAA rights
- If an employee (or covered dependent) complains his or her health plan privacy rights have been violated, the person complaining should be directed to the Privacy Officer, or if any employee wants to complain about a health plan privacy violation by someone else (including by your vendors), all those receiving such a complaint should make a written report to the Privacy Officer
- The HIPAA Policies must include forms for making privacy complaints
- All complaints should be investigated by the Privacy Officer
- Retaliation for making privacy complaints is prohibited

Employee Sanctions for Violations

- Employers are required by HIPAA to have and apply appropriate sanctions against the health plan's workforce who fail to comply with the plan's privacy policies and procedures or the privacy requirements of HIPAA
- In other words, if the members of the HR Department do not follow the HIPAA privacy policies they could be disciplined, up to and including termination of employment

Policies & Procedures

- HIPAA requires the establishment and maintenance of HIPAA Policies & Procedures
- All who handle PHI should retain a copy of the Policies & Procedures
- All who handle PHI should be familiar with the requirements of the Policies & Procedures

Safeguards for Hard-Copy PHI

- Clean desk rule—PHI should not be left out and unattended
- Dispose of material containing PHI by means of secure trash bins designated for shredding
- Do NOT use interoffice mail to transmit PHI
- Lock all file cabinets containing PHI

Safeguards for Oral PHI

- Only discuss PHI in your office or a conference room with the door closed
  - If you work in a cubicle area and must discuss PHI in your cubicle area, do not use identifiers and use appropriate volume
- Only discuss PHI with other authorized workforce members or business associates
- Remember—the minimum necessary rule applies

Safeguards for Emailing PHI

- Avoid using email to transmit PHI:
  - When transmitting e-PHI to a vendor, use a vendor secure website instead of email when possible
  - Upon receipt of an email with PHI from a participant which requires a response that contains PHI, respond by telephone to the extent possible
- If you must use email to transmit PHI:
  - do not use identifiers to the extent possible (in the message and the subject line);
  - delete the email chain below your message;
  - use caution regarding recipients (e.g., reply all); and
  - if the email must be sent outside the company, use encryption where possible

Safeguards for Electronic PHI

- Physical safeguards:
  - Computer screens should be out of sight from others – if you work in a cubicle, use a privacy screen
  - Log-off from your computer when you leave your workstation for any amount of time
  - Don’t save unencrypted files with PHI to your laptop hard drive
  - Create strong password and do NOT share them
  - Do NOT file PHI in the same files as any other employee HR information, including personnel records
- Never download PHI to your personal computer or send it to your personal email address

Privacy Breach

- A privacy breach can occur when information is
- Physically lost or stolen
  - Paper copies, films, tapes, electronic devices
- Misdirected by others
  - Verbal messages sent to or left with the wrong voicemail
  - Mislabeled mail
  - Misdirected email
  - Wrong fax number
  - Placed on intranet, website, Facebook, Twitter
  - Not using secure email
  - If data is not de-identified it is easy to have an inadvertent violation

Breach Notification Rules

- Notification Requirement Upon Breach of "Unsecured" PHI applies:
- PHI is "unsecured" if it is not rendered "unusable, unreadable, or indecipherable to unauthorized individuals"
- "Secured" PHI acts as a safe harbor
- An impermissible use or disclosure of PHI is presumed to be a reportable breach unless the covered entity or business associate, as applicable, demonstrates through a documented risk assessment that there is a low probability that PHI has been compromised
- Notice must be provided "without unreasonable delay" but in no event later than 60 days from discovery of the breach or the date breach reasonably should have been discovered

Breach Notification Rules

- The Omnibus Rule articulates four factors that a risk assessment must consider:
  - The nature and extent of the PHI (e.g., sensitivity of data, likelihood of re-identification);
  - The unauthorized person to whom the PHI was used/disclosed;
  - Whether the PHI was actually acquired or viewed; and
  - Mitigation efforts (e.g., encrypting data)

Breach Notification Rules

- Content of Notice
  - Brief description of what happened, date of breach, and date of discovery of breach (if known)
  - Types of unsecured PHI involved in breach (e.g., full name, SSN, DOB, home address, account number)
  - What individuals should do to protect themselves from potential harm from breach
  - Actions covered entity taking to investigate, mitigate losses, and protect against future breaches
  - How to find more information

Breach Notification Rules

- Nature of notification
  - If business associate discovers breach, must notify covered entity (i.e., the group health plan) so it can notify affected individuals
  - Previously, contractual obligation to disclose “security incidents;” now direct statutory notification obligation
  - Covered entity may contract with business associate to handle administrative details on its behalf; pay for notifying affected individuals

Breach Notification Rules

- If covered entity experiences breach, must give notice to affected individuals (at last known address) or by e-mail (if specified as preference)
- If contact information for individual insufficient or out of date, and if 10 or more individuals, notice must be posted on covered entity's website for 90 days or broadcast in local media and active toll free number for 90 days; if urgency required "because of possible imminent misuse," notice must be by telephone or other means, as appropriate
- If breach involves 500 or more individuals, must immediately notify HHS and prominent media outlet

When is a breach considered discovered for purposes of the notice deadline?

- A breach is considered “discovered” as of the first day that it is known (or reasonably should have been known) to the plan
- Employers have an obligation to report breaches they cause
- *This means it is critically important that you report to the Privacy Officer as soon as you think a breach MAY have occurred—The time to respond may start ticking at the time YOU discover the breach*

If something happened but you are not sure if it would be considered a breach, tell the Privacy Officer and the situation will be evaluated

Action Items

- Report breaches to HHS annually and keep internal logs of breaches
- Meet the safe harbor for treating PHI as “secured” or implement breach notice policies and procedures
- If applicable, amend and distribute HIPAA privacy notice with revised information; send copies to business associates
- As necessary, sign amended or new BA agreements
- Conduct HIPAA Audit of policies and procedures to honor requests and general compliance
- Update policies and procedures for marketing restrictions, minimum necessary standard
- Implement training

Questions?

Stacy H. Barrow

sbarrow@marbarlaw.com

(617) 830-5457