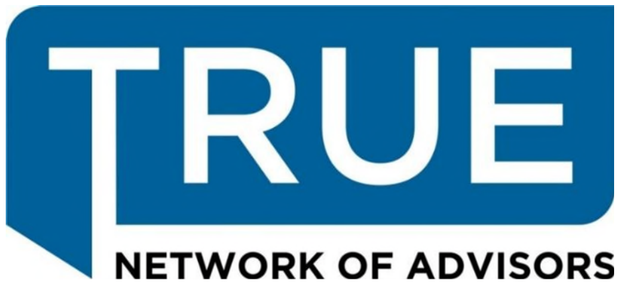
HIPAA Privacy and Security Training



Presented By:

Seth F. Capper
Maynard Nexsen PC

August 4, 2026

Agenda

1. Potential HIPAA Penalties
2. What Entities are Subject to HIPAA?
3. What is Protected Health Information (PHI)?
4. HIPAA Privacy Rule
5. HIPAA Security Rule
6. HIPAA Breach Notification Rules
7. Keys to HIPAA Compliance

HHS HIPAA Security Rule Guidance Materials for Professionals:
https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Potential HIPAA Penalties

Violation* Category	Amount of Penalty Per Violation	Maximum Penalty for All Violations of Identical Provision during Calendar Year
Did Not Know	$145 – $73,011	$2,190,294
Reasonable Cause	$1,461 – $73,011	$2,190,294
Willful Neglect, Timely Corrected	$14,602 – $73,011	$2,190,294
Willful Neglect, Not Timely Corrected	$73,011 (minimum penalty)	$2,190,294

Self-correction of violation within 30 days can be an affirmative defense to eliminate penalties

*Breaches of PHI are not necessarily violations, if plan's policies and procedures are followed appropriately, including plan's breach response procedures

*The numbers in the above table were published on January 28, 2026. Such penalties are adjusted by HHS from time to time to reflect changes in cost of living.

Entities Subject to HIPAA

HIPAA Covered Entities

- **Health Care Providers**
- **Health Insurance Companies**
- **Health Care Clearinghouses**
- **Health Maintenance Organizations (HMOs)**
- **Medicare, Medicaid, and Other Government Health Programs**
- **Employer-Sponsored Group Health Plans**
  - **Medical Plans**
  - **Dental Plans**
  - **Vision Plans**
  - **HRAs**
  - **Health FSAs**
  - **Wellness Programs**
  - **Disease Management Programs**
  - **Telemedicine Programs**
  - **EAPs**

<u>Business Associates</u>

Are not HIPAA covered entities, but they are subject to all of the same rules as covered entities (*i.e.*, downstream liability)

"Excepted Benefits" are <u>not</u> HIPAA covered entities (*e.g.*, disability insurance, accident-only insurance, on-site medical clinics)

“Hands Off” PHI Exception

- Extent to which HIPAA applies to an employer’s group health plans depends on the employer’s role in plan administration and whether the plan is self-funded or fully insured
- Most of HIPAA’s privacy rules do not apply if:
  - The plan is fully insured; and
  - The plan is “hands off” PHI
- A fully insured plan is considered to be “hands off” PHI if the plan does not create or receive PHI, other than summary health information and enrollment and disenrollment information

Business Associates

- **HIPAA applies to Business Associates (BAs)**
- **What is a BA?**
  - **External company or person performing functions on behalf of your Covered Entities (CEs) (*i.e.*, your health plans) that involve creating, receiving, maintaining, or transmitting PHI**
    - Examples: consultants, auditors, financial services, attorneys, administrators, utilization review, quality assurance, claims processing
- **Execute Business Associate Agreements (BAAs) before sharing PHI with service providers**
- **Subcontractors are also BAs:**
  - **A subcontractor that creates, receives, maintains, or transmits PHI on a BA's behalf is a BA in its own right**
  - **BAs must get assurances from their subcontractors**

Employers and HIPAA

- Employers (plan sponsors) are not Covered Entities (CEs); it is the group health plans that employers sponsor that are the CEs and that are subject to HIPAA
- Think about your group health plans as a separate legal entity from the employer
- The HIPAA rules limit the PHI that the group health plans may share with the employer to the following:
  1. De-identified information (which is not PHI)
  2. Enrollment / disenrollment information
  3. Summary health information for insurance placement purposes and settlor functions
  4. PHI shared pursuant to a signed individual authorization
  5. PHI shared for certain plan administration functions, if the plan document is amended and “firewall” is in place

What is PHI?

- Can be oral, written, or electronic information
- Three important characteristics:
  1. Created, received or maintained by or on behalf of CE or BA
  2. Health Information
     - Past, present, or future physical or mental health condition
     - Provision of health care to an individual, or
     - Past, present or future payment for the provision of health care to the individual
  3. Individually Identifiable Information
     - Health information from the plan is individually identifiable if there is a reasonable basis to believe that the information can be used to identify the individual
     - ***18 HIPAA Identifiers***
- ***What health info is not PHI?*** Employment records held by a CE in its role as employer; de-identified information

HIPAA Identifiers

The 18 Identifiers defined by HIPAA are:	
Name	Medical Record Number
Postal Address	Health Plan Beneficiary Number
All Elements of Date, Except Year	Device Identifiers and Serial Numbers
Telephone Number	Vehicle Identifiers and Serial Numbers
Fax Number	Biometric Identifiers (Finger & Voice)
Email Address	Full Face Photos and Comparable Images
URL Address	Any Other Unique Identifying Number, Code, or Characteristic
Social Security Number	IP Address
Account Numbers	License Numbers

HIPAA Privacy Rule

- **The HIPAA Privacy Rule requires CEs to:**
  - **Only use or disclose PHI as allowed under the Privacy Rule**
  - **Secure records containing PHI**
  - **Designate an individual to serve as Privacy Officer**
  - **Adopt and implement written HIPAA Privacy Policies and Procedures (to assist with workforce training and promote consistency in decisions involving individuals' PHI rights)**
  - **Notify individuals about their privacy rights and how their information can be used ("Notice of Privacy Practices")**
  - **Train employees so that they understand the CE's privacy policies and procedures, and develop a system to sanction employees for violations**

HIPAA Privacy Rule

Minimum Necessary Standard

Uses and Disclosures of PHI

The Privacy Officer

Policies & Procedures

Notice of Privacy Practices

Minimum Necessary Standard

- **CEs must reasonably ensure that any PHI used, disclosed, or requested is limited to the <u>minimum necessary to accomplish the intended purpose</u>**
- **Exceptions to the minimum necessary standard exist for:**
  - Uses or disclosures required by law
  - Disclosures to individuals who are the subject of information
  - Uses or disclosures for which the CE has received an authorization that meets certain requirements
- **<u>Incidental uses and disclosures permitted</u> if the CE has applied reasonable safeguards and implemented the Minimum Necessary Standard**

HIPAA Privacy Rule

Minimum Necessary Standard

Uses and Disclosures of PHI

The Privacy Officer

Policies & Procedures

Notice of Privacy Practices

Uses and Disclosures of PHI

HIPAA Privacy Rule

Minimum Necessary Standard

Uses and Disclosures of PHI

The Privacy Officer

Policies & Procedures

Notice of Privacy Practices

- **Permitted uses and disclosures (without individual authorization):**
  - Disclosure to the individual
  - Uses and Disclosures required or permitted under HIPAA's public policy exceptions
  - Disclosure to family members or close personal friends, with respect to limited types of information, if the individual has an opportunity to agree or object
  - Uses and Disclosures for <u>treatment, payment, or health care operations</u>
    - Encompasses the vast majority of day-to-day uses and disclosures
    - Includes Uses and Disclosures for health plan underwriting purposes
- **Uses and disclosures that are not otherwise permitted under the rules require an <u>individual authorization</u>**
  - *<u>Never</u> access or use PHI from the health plans for employment purposes that are not related to plan administration*

The Privacy Officer

- CEs must designate a privacy officer who is responsible for development and implementation of the CE's policies and procedures and a contact person (the privacy official or another person) for receiving complaints and providing additional information concerning the privacy notice
- A CE's HIPAA privacy officer:
  - Is the "buck stops here" representative regarding the CE's privacy-related compliance
  - A CE with multiple subsidiaries that are CEs in their own right may consider itself to be one CE for purposes of designating a privacy officer

HIPAA Privacy Rule

Minimum Necessary Standard

Uses and Disclosures of PHI

The Privacy Officer

Policies & Procedures

Notice of Privacy Practices

Policies & Procedures

- **CEs must adopt policies and procedures for PHI that are designed to comply with the Privacy Rule:**
  - **A CE's privacy officer is responsible for developing and implementing the CE's policies and procedures**
  - **This requirement is intended to assist with workforce training and promote consistency in decisions involving individuals' privacy rights (*e.g.*, access to PHI about them)**
  - **For example, a CE's policy should address who determines when information is withheld from an individual**
  - **A CE's policies and procedures (and, if applicable, its notices of privacy practices) must be updated to comply with changes in the law**

HIPAA Privacy Rule

Minimum Necessary Standard

Uses and Disclosures of PHI

The Privacy Officer

Policies & Procedures

Notice of Privacy Practices

Policies & Procedures

- **The Privacy and Security Policies and Procedures serve as the organization's written HIPAA compliance manual and generally include:**
  - **Privacy (PHI) Use and Disclosure Policies**
  - **Individual Rights and Authorization Forms**
  - **Plan Sponsor Certification**
  - **Notice of Privacy Practices**
  - **Appointments of Privacy and Security Officials and descriptions of such roles/responsibilities**
  - **Business Associate Agreements**
  - **Breach Assessment and Notification Policies**
  - **Separate Security Policies and Procedures**

HIPAA Privacy Rule

Minimum Necessary Standard

Uses and Disclosures of PHI

The Privacy Officer

Policies & Procedures

Notice of Privacy Practices

Notice of Privacy Practices

- **CEs must distribute a Notice of Privacy Practices (*aka*, "Privacy Notice") that describes**:
  - The uses and disclosures of PHI a CE is allowed to make for treatment, payment, or health care operations (and for any other purposes without an individual's authorization)
  - The CE's legal duties and privacy practices regarding PHI
  - The individual's rights regarding PHI (*e.g.*, an individual's right to inspect, copy, and amend PHI)
  - The CE's obligation to notify individuals following a breach of unsecured PHI
  - An individual's ability to make a complaint to the CE or to HHS if the individual thinks his or her privacy rights were violated

HIPAA Privacy Rule

Minimum Necessary Standard

Uses and Disclosures of PHI

The Privacy Officer

Policies & Procedures

Notice of Privacy Practices

Notice of Privacy Practices

- **To whom must the Privacy Notice be provided?**
  - **Anyone who requests it**
  - **Individuals covered by the plan – single notice to the named insured or covered employee is effective for all dependents**
- **Distribution requirements for Privacy Notices**:
  - **Health plans must provide Privacy Notice**–
    - To new enrollees, upon enrollment
    - Within 60 days of a material change to the notice, to individuals who are covered under the plan
  - **At least once every three years, health plans must inform covered individuals:**
    - Of the Privacy Notice's availability upon request and how to obtain it

HIPAA Privacy Rule

Minimum Necessary Standard

Uses and Disclosures of PHI

The Privacy Officer

Policies & Procedures

Notice of Privacy Practices

HIPAA Privacy: Individual Rights

- The Privacy Rule provides individuals the rights to:
  - Access and make copies of the individual's PHI held in a designated record set
  - An accounting of disclosures of PHI
  - Have changes made to errors in the individual's designated record set
  - Request additional restrictions on the use of PHI
  - Request a preferred means of communications
  - Make complaints about the CE's HIPAA policies and procedures
  - Not be retaliated against for exercising HIPAA rights

HIPAA Security Rule

- Applies to Electronic PHI (“ePHI”)
- Protects the confidentiality, integrity, and availability of ePHI when it is received, maintained, or transmitted
  - CEs must comply with Security Rule if they transmit ePHI
  - Under the HITECH Act, BAs also must comply
- The Security Rule is organized into three general categories of “safeguards”:
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
- CE must perform a ***risk analysis*** to determine potential risks and which security measures to adopt based on what is reasonable and appropriate for CE’s circumstances

HIPAA Security: Implementation Specifications

Administrative	Physical	Technical

• HIPAA Program
• Risk Analysis
• Workforce Authorization and Supervision
• Training
• Incident Response
• Sanctions
• Contingency Plan
• Consider additional policies addressing:
  o Confidentiality
  o Removable Media
  o Personal Mobile Devices
	• Workstation Use and workstation security
	• Facility Access Controls
	• Employee Authorizations
	• Visitor Policies
	• Equipment Control (into and out of a worksite)
	• Locks on Doors, Containers, Cabinets
	• Shredding / Disposal
	• Monitor Printers
	• Separate Files
	• Alarms
		• Audit Controls
		• Access Control
		• Unique User Identification
		• Integrity
		• Person or Entity Authentication
		• Transmission Security
		• Password Protections
		• Encryption and Decryption (Addressable)
		• Emergency Access Control
		• Limited Access
		• Automatic Logoff
		• Separate Files
		• Data Backup

! BREACH !

- **Breach means:**
  1. The acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule
  2. Which compromises the security or privacy of the PHI
- **What if you discover a potential breach?**
  - Take action as soon as possible – mitigate the breach and its effects, and report the breach to the Privacy and Security Officer
  - Follow the Breach Notification Policies and Procedures
  - Determine whether there has been an impermissible use or disclosure of unsecured PHI (*i.e.*, determine whether an exception applies; conduct a risk assessment). Remember, documentation is key.
- **<u>Risk Assessment</u> – Presumption that PHI was "Compromised"**
  - Any breach is presumed to be at a level which "compromises" the security or privacy of the PHI, ***<u>unless</u>*** <u>a risk assessment</u> determines there is a "<u>low probability</u>" that the PHI has been compromised

! BREACH !

Risk Assessment Factors

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated
- Any other relevant factors

Breach Exceptions

- **<u>Exceptions to the definition of a breach</u>**:
  - **The unintentional acquisition, access, or use of PHI by an employee if**:
    - **Made in good faith and within the scope of the individual's employment**
    - **There is no further use or disclosure of the PHI in an impermissible manner**
  - **Inadvertent disclosures of PHI from one authorized person to another**
  - **Disclosures of PHI if the CE or BA has a good faith belief that the unauthorized person to whom the disclosure was made could not reasonably retain the information**

Breach Notification

- **Notification required when there is a breach of unsecured PHI**
- **Under the Breach Notification Rules:**
  - CEs must provide notice of a breach to individuals, HHS, and, for large breaches, to the media
  - BAs must provide notice of a breach to CEs
- **Notification Timing**:
  - A breach is treated as discovered on first day it is known, or would have been known with the exercise of reasonable diligence
  - Report all breaches to affected individuals within 60 days of discovery
  - Small Breaches (affecting <500 individuals): Enter in log and report log to HHS within 60 days after end of the calendar year
  - Large Breach (affecting 500+ individuals):
    - Report immediately to HHS (no later than 60 days after discovery)
    - If breach affects 500+ residents of a single state, report immediately to prominent media outlets in that state (no later than 60 days after discovery)

Keys to HIPAA Compliance

- **<u>HIPAA Golden Rules</u>:**
  - **Minimum Necessary Standard**
    - Limit use and disclosure of PHI to the minimum necessary required to accomplish the intended purpose
  - **Firewalls**
    - Do not use PHI for employment purposes or decisions
  - **Follow HIPAA Privacy and Security Policies and Procedures**
  - **Documentation**
  - **Execute Business Associate Agreement <u>*before*</u> disclosing PHI**
- **<u>Avoidance</u>: Seek to limit your access to and disclosure of PHI (*e.g.*, if possible, request that info from internal systems or Business Associates not include personal identifiers)**
- **<u>HIPAA Training</u>: You!**

"An ounce of prevention is worth a pound of cure."

– HHS Office of Civil Rights Director

TRUE

NETWORK OF ADVISORS

MAYNARDNEXSEN

HIPAA TRAINING CERTIFICATION

By my signature, I hereby certify that I have completed the HIPAA training course for my organization and its group health plans.

_____

Signature

_____

Print Name

Date: _____