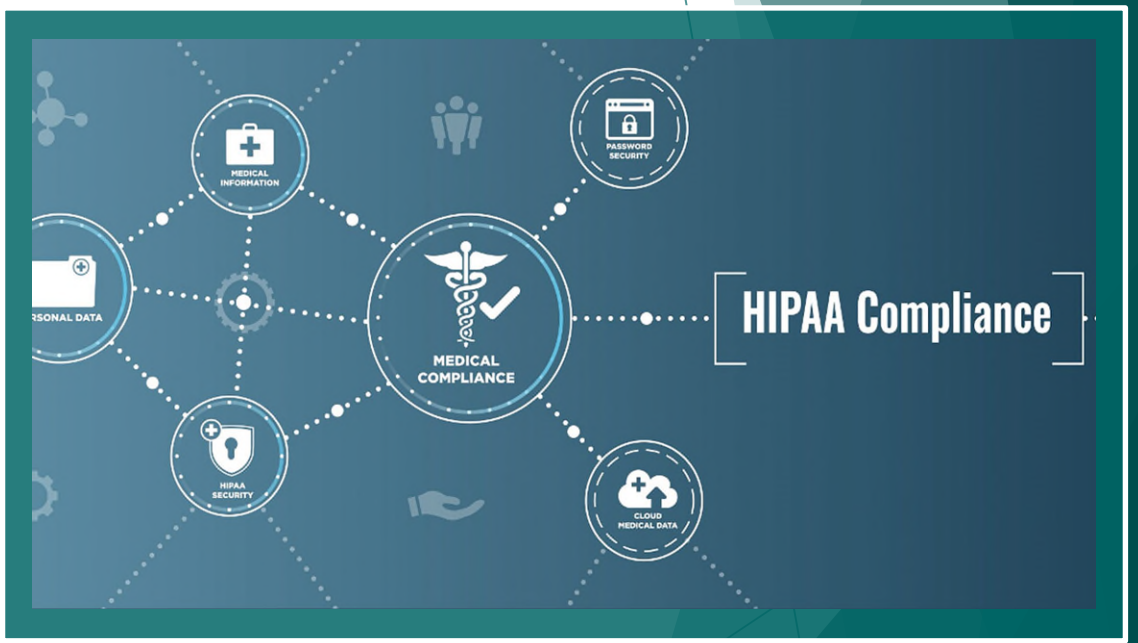
HIPAA Privacy and Security Training

Presented By:
Seth F. Capper
Maynard Nexsen PC
May 9, 2023

Best Lawyers RATED BY Super Lawyers

Agenda

- HIPAA and HITECH 101
- Who is subject to HIPAA, and what information is protected?
- Substantive requirements:
  - Privacy Rule
  - Security Rule
  - Breach Notification
- HIPAA Compliance Program
- Strategy and Golden Rules



MAYNARDNEXSEN

Potential Penalties

Breach/Violation Category	Amount of Penalty Per Violation	Maximum Penalty for All Violations of Identical Provision during Calendar Year
Did Not Know	$127 – $63,973	$1,919,173
Reasonable Cause	$1,280 – $63,973	$1,919,173
Willful Neglect, Timely Corrected	$12,794 – $63,973	$1,919,173
Willful Neglect, Not Timely Corrected	$63,973 (minimum penalty)	$1,919,173

*The numbers in the above table are for 2022. Such penalties are adjusted by HHS from time to time to reflect changes in cost of living.

MAYNARDNEXSEN

HIPAA and HITECH 101

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Protects the privacy of Protected Health Information (PHI)
  - Provides for electronic and physical security of PHI
  - Requires “minimum necessary” use and disclosure
  - Specifies Individual Rights with regard to access and control over the use of their PHI
- Changes under the Health Information Technology for Economic and Clinical Health (HITECH) Act (2009)
  - Breach notification requirements
  - Fine and penalty increases for privacy violations
  - Provides for “downstream” liability
  - Department of Health and Human Services (HHS) audits
- Comprehensive final regulations (January 2013)

MAYNARDNEXSEN

Entities Subject to HIPAA

HIPAA Covered Entities (CEs)*

- **Health plans**
- **Health care clearinghouses**
- **Health care providers who conduct certain health care transactions in electronic form (e.g., fund transfers)**

*__Business Associates (BAs)__ are also subject to virtually to same rules as Covered Entities (CEs)

For HIPAA purposes, health plans include

- **Health insurance companies**
- **Health maintenance organizations (HMOs)**
- **Medicare, Medicaid, other gov't programs**
- **Employer-sponsored group health plans (medical, dental, vision, health FSA, wellness programs, EAPs, etc.)**

MAYNARDNEXSEN

Business Associates

- HIPAA applies to a CE's "Business Associates" (BAs)
  - A BA is an entity that performs certain functions that involve creating, receiving, maintaining, or transmitting PHI, on behalf of a CE
    - PHI is the key
    - Examples: consultants, auditors, financial services, attorneys, administrators, utilization review, quality assurance, claims processing
- Establish Business Associate Agreement (BAA) before providing PHI
- 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

MAYNARDNEXSEN

Employers and HIPAA

- Employers (*i.e.*, plan sponsors) are not Covered Entities (CEs); group health plans that employers sponsor are the CEs
- Extent to which HIPAA applies to the employer's group health plan 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 to fully insured plans that are "hands off" PHI
- The rules limit the PHI that a group health plan may share with the employer/plan sponsor
  - De-identified information (which is not PHI)
  - Enrollment/disenrollment information
  - Summary health information for insurance placement purposes and settlor functions
  - Pursuant to a signed authorization
  - For certain plan administration functions, if plan document is amended and "firewall" is in place

MAYNARDNEXSEN

What is PHI?

- Can be oral, written, or electronic information
- <u>Three important characteristics</u>:
  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

MAYNARDNEXSEN

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 and Voice Prints)
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

MAYNARDNEXSEN

HIPAA Privacy Rule

- The HIPAA Privacy Rule requires CEs to:
  - Notify individuals about their privacy rights and how their information can be used (“Notice of Privacy Practices”)
  - Adopt and implement privacy policies and procedures
  - Train employees so that they understand the CE's privacy policies and procedures, and develop a system to sanction employees for violations
  - Designate an individual (“Privacy Officer”) to ensure that the CE's privacy procedures are adopted and followed (a similar requirement applies under the HIPAA Security Rule)
  - Secure records containing PHI
  - Only use or disclose PHI as allowed under the Privacy Rule

MAYNARDNEXSEN

HIPAA Privacy: Permitted Uses & Disclosures

- Use: Sharing, application, utilization, or analysis *within* a CE
- Disclosure: Release, transfer, provision of access to, or divulging in any other manner of information *outside* the CE

- General Rule: No use or disclosure of PHI unless permitted or required by the Privacy Rules or the rules concerning compliance and enforcement
  - Mandatory Disclosures
    - To the individual for access and accounting
    - To the Department of Health & Human Services ("HHS") for compliance and enforcement
  - Permitted Uses and Disclosures

MAYNARDNEXSEN

HIPAA Privacy: Permitted Uses & Disclosures

Minimum Necessary Standard (MNS)

- CEs must reasonably ensure that any PHI used, disclosed, or requested is limited to the minimum necessary to accomplish the intended purpose
- 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
- Incidental uses and disclosures permitted if the CE has applied reasonable safeguards and implemented the MNS

MAYNARDNEXSEN

HIPAA Privacy: Permitted Uses & Disclosures

- Disclosure with permission:
  - In the form of an individual authorization
- Disclosures without permission:
  - To the individual
  - To family members or close personal friends, with respect to limited types of information, if the individual has an opportunity to agree or object
  - As required or permitted under HIPAA's public policy exceptions
  - For treatment, payment, or health care operations

MAYNARDNEXSEN

HIPAA Privacy: 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

MAYNARDNEXSEN

HIPAA Privacy 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 (*e.g.*, the 2013 final regulations)

MAYNARDNEXSEN

HIPAA Privacy: Notice of Privacy Practices

- CEs must distribute a Notice of Privacy Practices (NPP) 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

MAYNARDNEXSEN

HIPAA Privacy: Notice of Privacy Practices

- To whom must the NPP 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 NPPs:
  - Health plans must provide NPPs:
    - 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 NPP's availability and how to obtain it

MAYNARDNEXSEN

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 any HIPAA rights

MAYNARDNEXSEN

HIPAA Security Rule

- Applies to ePHI (e.g., PHI in emails, or PHI stored on computers or jump-drives)
- 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
- Must perform ***risk analysis*** to determine which security measures to adopt based on what is reasonable and appropriate

MAYNARDNEXSEN

HIPAA Security Rule

- The HIPAA Security Rule requires CEs to:
  - Adopt reasonable and appropriate policies and procedures to ensure compliance with the Security Rule
  - Keep all documents for six years from the later of the date (1) they were created or (2) when they were last in effect
  - Make the documents available to employees who are responsible for implementing the policies and procedures
  - Maintain a written record of any action, activity, or assessment required to be documented by the Security Rule
  - Review and update documents periodically for changes (environmental or operational) affecting the security of ePHI
  - Like under the Privacy Rule, designate a Security Officer (which may be the same or a different person than the Privacy Officer)

MAYNARDNEXSEN

HIPAA Security: Compliance Safeguards

Administrative	Physical	Technical

• HIPAA Program
• Day-to-day operations
• Training
• Sanctions
• Consider additional policies:
  • Confidentiality Policy
  • Removable Media Policy
  • Personal Mobile Device Policy
	• Workstation use and workstation security
	• Facility Access Controls
	• Only authorized employees
	• Sign-in for visitors and escorts
	• Equipment control, into and out of a worksite
	• Lock doors, containers, cabinets
	• Shred PHI
	• 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 log off
		• Separate files
		• Data back up

HIPAA Security: Administrative Safeguards

- Comprise most of the Security Rule's standards
- Involve administrative functions for implementing, managing, and maintaining security measures to protect ePHI
- Administrative safeguard example: Security Incidents
  - CEs must develop policies and procedures to address security incidents, which are defined as:
    - An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information
    - Interference with information systems
  - Specific examples of security incidents include:
    - Stolen passwords used to access ePHI
    - Physical theft or loss of electronic media
    - Virus attacks affecting the operation of information systems containing ePHI

MAYNARDNEXSEN

HIPAA Security: Physical Safeguards

- Requirements to protect a CE's or BA's electronic information systems and ePHI from unauthorized physical access
- Entities must limit physical access to ePHI while permitting properly-authorized access
- The specific physical safeguard standards are:
  - Facility access controls
  - Workstation use
  - Workstation security
  - Device and media controls

MAYNARDNEXSEN

HIPAA Security: Technical Safeguards

- Involve the technology, policies, and procedures that protect ePHI and control access to it
- Specific technical safeguard standards are:
  - Audit controls
  - Access controls
  - Integrity (i.e., protection of ePHI from improper alteration or destruction)
  - Person or entity authentication
  - Transmission security

MAYNARDNEXSEN

! BREACH !

- Breach means…
  - the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule
  - which compromises the security or privacy of the 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
- Presumption of "Compromise"
  - Any breach is presumed to be at a level which "compromises" the security or privacy of the PHI
  - UNLESS a risk assessment determines there is a "low probability" that the PHI has been compromised

MAYNARDNEXSEN

! 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
  - Other relevant factors

MAYNARDNEXSEN

HIPAA Breach Notification: Exceptions

Exceptions to the definition of a breach exist for:

- **The unintentional acquisition, access, or use of PHI by an employee if:**
  - **Made in good faith and within the employee's authority**
  - **There is no further use or disclosure of the PHI**
- **Certain inadvertent disclosures of PHI**
- **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**

MAYNARDNEXSEN

HIPAA Breach Notification

- Follow Breach Notification Policies and Procedures
  - Report to Privacy and Security Officer
  - Mitigate the breach and effects of the breach to the extent possible
- Determine whether there has been an impermissible use or disclosure of unsecured PHI; determine whether an exception applies; conduct a risk assessment – documentation is key
- Notification required when there is a breach of unsecured PHI
- Timing
  - It is important to take action on potential breach as soon as possible
  - Breach is treated as discovered on first day it is known or should have been known (with exercise of reasonable diligence)
- Report breach to individuals – within 60 days of discovery
  - HHS Log: 60 days after end of the calendar year
  - Large breaches (affecting 500+ individuals): Media and HHS

MAYNARDNEXSEN

HIPAA Compliance Program

- Compliance Program Materials
  - Privacy and Security Policies and Procedures
    - Proper Use and Disclosure
    - Breach Risk Assessment and Notification Procedures
  - Authorizations
  - Plan Sponsor Certification
  - Notice of Privacy Practices
- Administrative, Physical, and Technical Security Safeguards
- You!

MAYNARDNEXSEN

HIPAA Golden Rules

- Minimum Necessary Standard
  - Limit use and disclosure of PHI to the minimum necessary required to accomplish the intended purpose
- Firewalls
  - May not use PHI for employment purposes or decisions
- Follow HIPAA Privacy and Security Policies and Procedures
- Documentation
- Remember: Business Associate Agreement BEFORE disclosing PHI

> ***"An ounce of prevention is worth a pound of cure."***
>
> – HHS Office of Civil Rights Director

MAYNARDNEXSEN

PHI Strategy: Avoidance

- Seek to limit your access to and disclosure of PHI
- Avoidance is consistent with Minimum Necessary Standard obligations
  - Request that information from Insurers, TPAs, Business Associates not contain personal identifiers
  - Reject broad requests for information containing PHI
  - Monitor info and recognize PHI that requires protection
- De-Identified or Limited Data Set – excludes HIPAA identifiers
- If you receive PHI erroneously:
  - Inform provider that info provided contains PHI
  - Document actions you took with regard to PHI
  - Request the info in a form without PHI

MAYNARDNEXSEN

HIPAA TRAINING CERTIFICATION

By my signature, I hereby certify that I have reviewed the HIPAA Training PowerPoint presentation.

_____

Signature

_____

Print Name

Date: _____