



Risk & Insurance | Employee Benefits | Retirement & Private Wealth

HIPAA Compliance for Group Health Plans

Understanding the Rules, Regulations and Obligations

Fall 2024



Dennis Fiszer, Esq.

Senior Vice President, Employee Benefits
Compliance Practice Leader

HUB International



Dawn Smith, JM, SHRM-CP, MSA

Employee Benefits Compliance Manager

HUB International



Shelly Hodges-Konys

Director, Group Compliance Benefits

HUB International

Agenda

- 1 | HIPAA Foundational Principles
- 2 | HIPAA Privacy & Security Standards
- 3 | HIPAA HITECH Act

HIPAA Foundational Principles



Enforcement and Penalties

Violation Category	Each Violation	Violations of an Identical Provision in Calendar Year
Did Not Know	\$137–\$68,928	\$2,067,813
Reasonable Cause	\$1,379–\$68,928	\$2,067,813
Willful Neglect, Corrected w/in 30 days	\$13,785–\$68,928	\$2,067,813
Willful Neglect, Not Corrected w/in 30 days	\$68,928–\$2,067,813	\$2,067,813

What is HIPAA and Who Has Enforcement Authority?

HIPAA - the **Health Insurance Portability and Accountability Act**

Federal law enacted in 1996 as an attempt at incremental healthcare reform

Regulated by The Department of Health and Human Services (HHS) and enforced by the Office of Civil Rights

Intent - to reform the healthcare industry by reducing costs, simplifying administrative processes and burdens, and improving the privacy & security of patients' information

Prior to the ACA, considered the most significant healthcare legislation since Medicare in 1965



What Does HIPAA Do?

- **Requires protection, confidentiality and data integrity of Protected Health Information (PHI) including:**
 - Verbal discussions (i.e., in person or on the phone)
 - Written (i.e., emails, faxes, copies, Explanation of Benefits, notes, etc.)
 - Computer systems and applications (i.e., electronic files or cloud system storage, mobile devices, laptops, copier and computer hard drives, etc.)
- **Prevents unauthorized use and disclosure of PHI**
 - Use – when reviewing or discussing PHI internally (audits, training, customer service, quality control)
 - Disclosure – release/distribution of someone else's PHI to a third party without the permission of the person who owns the PHI (i.e., carriers, employers, etc.)
- **Establishes Privacy rights**
- **Establishes Security standards**
 - Structures how carriers, employer groups and others handle, receive, and use PHI



What type of information is Protected by HIPAA?

- **Health Information (HI)** - information, whether oral or communicated in any medium, that relates to an individual's medical condition, the provision of medical care for that individual, or the payment for that individual's medical care
 - Includes health coverage enrollment, premium payment information, and information relating to medical conditions and treatment
- **Individually Identifiable Information (III)** - information that identifies (or could reasonably be used to identify) the individual to whom it relates and is created or received by a covered entity or an employer

















Protected Health Information (PHI)= HI + III

- PHI does not include information contained in educational records, employment records, and/or regarding a person deceased for more than 50 years.


**HEALTH INFORMATION MAINTAINED AS PART OF EMPLOYMENT RECORD IS EXEMPTED...
BUT OTHER STATE PRIVACY LAWS MAY APPLY TO THESE.**

Individually Identifiable Information

Identifiers in Protected Health Information that can be linked back to an individual:

 Name, Last Name	 Address	 E-mail	 Account Number
 Dates of birth and other dates that relate to an individual	 Driver's License Number	 VIN (Vehicles)	 Photographs
 Medical Record Number	 Health Plan Beneficiary Number	 Social Security Number	 Telephone Numbers
 URLs	 IP Addresses	 Biometric ID	 Other Unique Identifiers

Who Must Comply? Covered Entities

Healthcare Providers* 	Health Plans 	Healthcare Clearinghouses 
<ul style="list-style-type: none">○ Physicians○ Dentists○ Nurses○ Psychologists○ Pharmacies○ Clinical Laboratories○ Nursing homes○ DME suppliers <p><i>*Only if they transmit any information in an electronic form in connection with a transaction for which HIPAA has adopted a standard</i></p>	<ul style="list-style-type: none">○ Health insurance companies○ HMOs○ <i>Employer group health plans</i>○ Government programs that pay for healthcare:<ul style="list-style-type: none">– Medicare– Medicaid– Military and Veterans Healthcare Programs	<ul style="list-style-type: none">○ Entities that process nonstandard health information they receive from another entity into a standard format (i.e., standard electronic format or data content), or vice versa.○ Clearinghouse examples include entities offering billing, claims processing, ICD9 coding and eligibility verification services○ In service to a health plan, it may also be a Business Associate

Who Must Comply? **Business Associates**

Business Associates are third-party vendors and business partners that create, receive, maintain, or transmit protected health information (PHI) on behalf of a Covered Entity.

Examples of Business Associates include:



Third Party Administrators



Insurance Brokers and consultants



Wellness Vendors



Actuaries



Accountants



Consultants



Asset Recyclers



IT Consultants

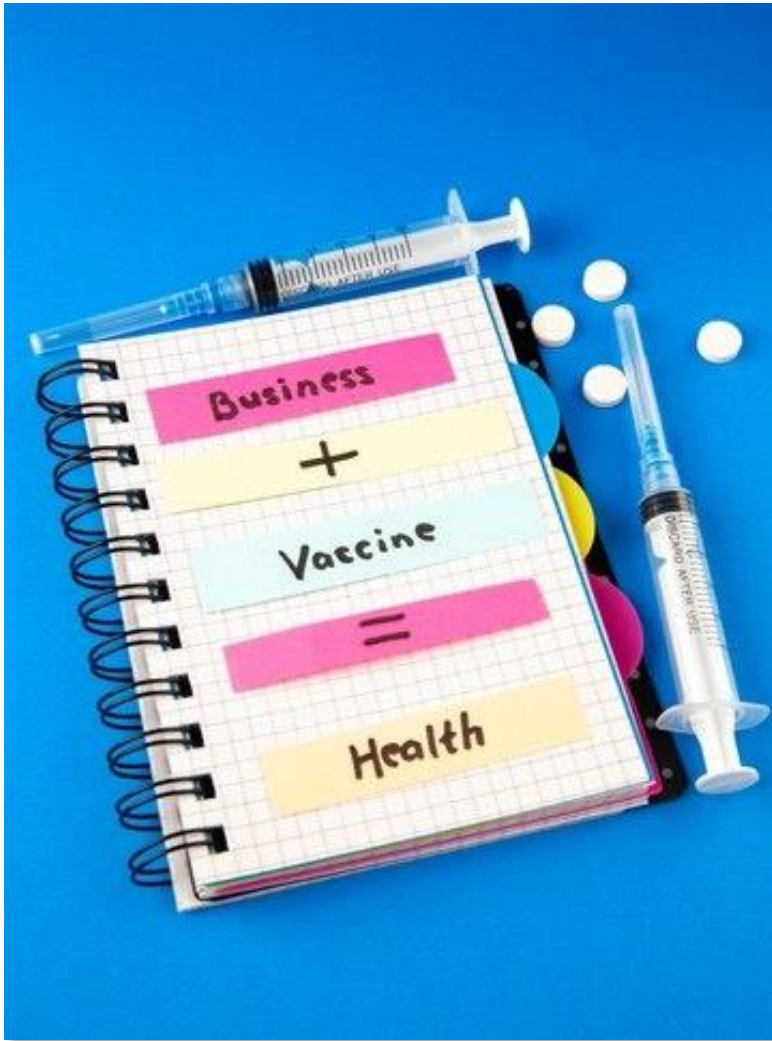


Claims Processing



Software Companies

Covered Health Plans



Almost all employer group health plans (both fully insured and self insured) that provide or pay for medical care for employees or their dependents are expected to comply with HIPAA.

- Medical Benefit Plans
- Prescription Drug Plans
- Dental Plans
- Vision Plans
- Wellness Programs
- Employer On-Site Health Clinics
- Employee Assistance Programs (EAPs)
- Section 125 (Flexible Spending Accounts)
- Cafeteria Plans with Medical Care Options

Exempt Health Plans and Excepted Benefits

Exempt Group Health Plans		
Have fewer than 50 participants	&	Are self-insured and self-administered by the employer

Certain types of insurance benefits (i.e., property/casualty insurance etc.), under which benefits for medical care are secondary or incidental to other insurance benefits. **Excepted Benefits** includes but is not limited to:

- Life Insurance
- **Workers' Compensation**
- Accidental Death & Dismemberment
- Short- & Long-Term Disability
- Automobile Insurance
- Reinsurance/Stop Loss
- Prescription Discount Programs
- Other Non-Health Related Benefits (i.e., FMLA)

HIPAA Privacy & Security Standards



Difference Between Privacy and Security



1. Right of an individual to control the use of his or her PHI
2. Sets the standards for how PHI should be controlled
3. Covers safeguarding of PHI in ALL forms from unauthorized disclosure



SECURITY rule establishes standards for safeguarding of PHI in electronic form (ePHI) from unauthorized disclosure, destruction, or loss.

Privacy depends in part on Security measures to ensure confidentiality.

Components of a Privacy Program



The Privacy Policy

01

Provide individuals with a clearly written explanation of how their medical information will be used, kept and disclosed

02

Individuals have the right to request access, copy, and request amendments to their PHI

03

Individuals have the right to request an accounting of disclosures made other than for treatment, payment or healthcare operations

04

Disclosure of an individual's health information must be limited to the minimum necessary to comply with the request

05

Criminal and civil sanctions for improper use or disclosure of PHI

06

Requirements for access to records by researchers and others

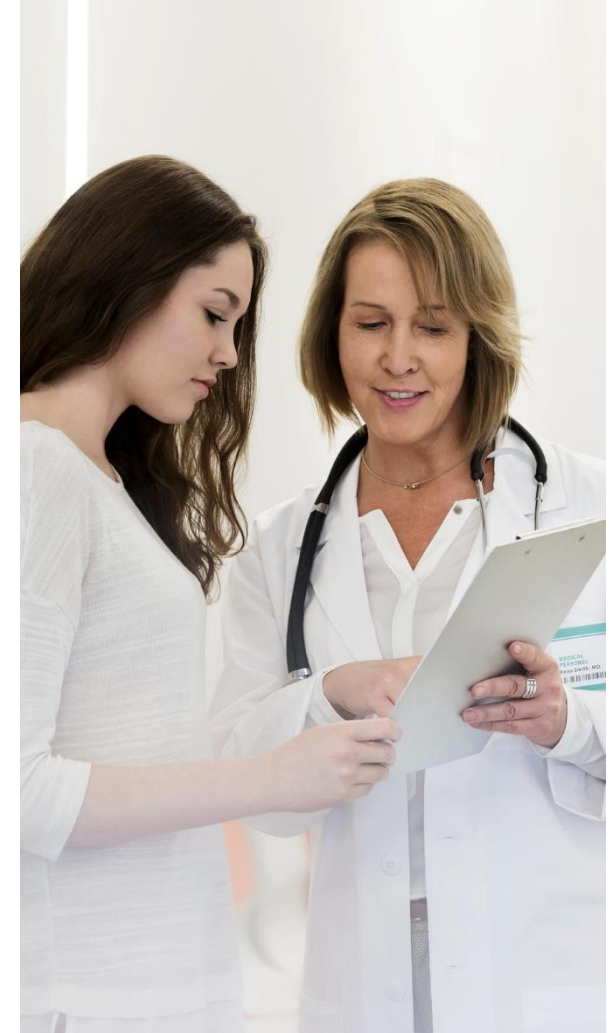
07

Covered entities must establish written policies documenting compliance with the privacy standards

Notice of Privacy Practices

Information regarding a plan participant's privacy rights and written notice of the PHI use and disclosure policies of the group health plan:

- Health Plan must provide the notice to all current plan participants, all new plan participants at the time of enrollment, and upon request
- Is not required to provide the notice if health benefits are provided through an HMO or Health Insurance Issuer (*as HMO/Issuer will be responsible for providing the notice*)
- Must provide a notice to all individuals in the plan within sixty days of making any material change to the notice and must remind plan participants at least once every three years of the availability of the notice and the means to obtain it
- Must include a statement in the **Notice of Privacy Practices** indicating that PHI may be disclosed to the plan sponsor (the employer) for specific uses and with certain restrictions
- Must be posted on the plan sponsor's website if website is available
- May distribute the notice electronically if the individual consents



Distinction Between Health Plan and Plan Sponsor

- Important distinction between a **Group Health Plan** and the group health **Plan's Sponsor** (the employer)
- **Group Health Plan is its own separate legal entity and distinct** from the employer sponsoring it (i.e., the **Plan Sponsor**) for HIPAA purposes
- As such, both entities have a different status and set of responsibilities under HIPAA:
 - A **Group Health Plan** is considered a **Covered Entity** under HIPAA
 - Employers themselves are **NOT** considered Covered Entities under HIPAA, but because the employer is involved in the operation of the group health plan and has access to PHI, it absorbs responsibility for many employer specific HIPAA privacy functions



Disclosures to the Plan Sponsor (Employer)

Plan Sponsor's privacy responsibilities **change depending on whether** the plan sponsor receives "Protected Health Information" **or** merely "Summary Health Information"

PHI may be disclosed to the Plan Sponsor only if:

- The plan documents have been amended to inform plan participants of the circumstances under which a disclosure would occur
- The plan sponsor provides an assurance in the form of a "certification" to the plan that the plan documents have been amended and it will:

Not use the PHI it receives for employment or other benefit purposes

Assist in the implementation of the amendment, access, and accounting rights

Ensure that adequate separation between the plan and plan sponsor is in place

Make records available to the Department of Health and Human Services

Provide for adequate separation between the health plan and others in the work force

Use the PHI it receives for plan administration purposes only

Disclosures to the Plan Sponsor (Employer)

Permissible disclosures and methods of disclosing PHI to the plan sponsor (employer):

- **Enrollment and Disenrollment Information**
- **De-identified Information** – PHI where all individually identifiable information has been removed
- **Authorization** – must comply with HIPAA authorization rules (we will review)
- **Summary Health Information (SHI)** – a subset of PHI from which individually identifiable information has been deleted (5-digit zip code may be used)



- **Summary Health Information** may **only** be used for:
 - Soliciting premium bids for health insurance coverage
 - Modifying, amending, or terminating the health plan

Permissible Uses and Disclosures of PHI

- Group health plans may use and disclose participants' PHI for purposes of TPO (***Treatment, Payment, and healthcare Operations***) – otherwise must obtain explicit authorization from each affected plan participant whose information will be used or disclosed.
- Examples of uses and disclosures for TPO for which an authorization is **NOT** required:
 - Determination of eligibility or coverage
 - Emergencies involving imminent threat to health or safety
 - Billing
 - Adjudication of claims and claims management
 - Healthcare data processing
 - Utilization review (including pre-certifications)
 - Medical necessity determinations
 - Workers Compensation
 - Underwriting and premium rating
 - Organ transplants/procurement
 - Conducting quality assessments (case management)
 - Evaluation of health plan performance
 - Arrangement for legal, auditing, or actuarial services
 - Business planning/certain administrative activities
 - Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits

Authorizations

Covered group health plans must obtain a plan participant's authorization for uses or disclosures other than TPO (*Treatment, Payment, and healthcare Operations*)

Example: Adding benefits, renewing, replacing, or amending coverage, placing contracts for excepted benefits, or marketing other products or services.

Authorization **must** describe the intended use or disclosure in specific terms - cannot be combined within a privacy notice.

For the majority of cases, a standard non-conditional authorization will be used in which a group health plan cannot condition the plan participant's enrollment or eligibility for benefits on receipt of a signed authorization.

02

Non-Conditional

Two
Types of
Authorizations:

Conditional

01

In limited circumstances, a group health plan can condition enrollment or eligibility for benefits on receipt of a signed authorization. This conditional type of authorization can ONLY be used PRIOR to an individual's enrollment in the plan and ONLY for purpose of making eligibility, underwriting, or risk rating determinations.

Assisting Employees with Claim Adjudication

01



It is very common for employees (i.e., HR) working on behalf of group health plans to assist plan participants with claims issues/processing

02



Claim adjudication records are considered PHI and the group health plan should have the proper safeguards for PHI in place as part of its HIPAA compliance program



Caution

Group health plans that opt to receive SHI (reducing its compliance requirements) generally do not have HIPAA PHI programs and must obtain a signed authorization from the plan participant before an employee working on behalf of the group health plan can assist with claims issues/processing

Minimum Necessary Disclosure



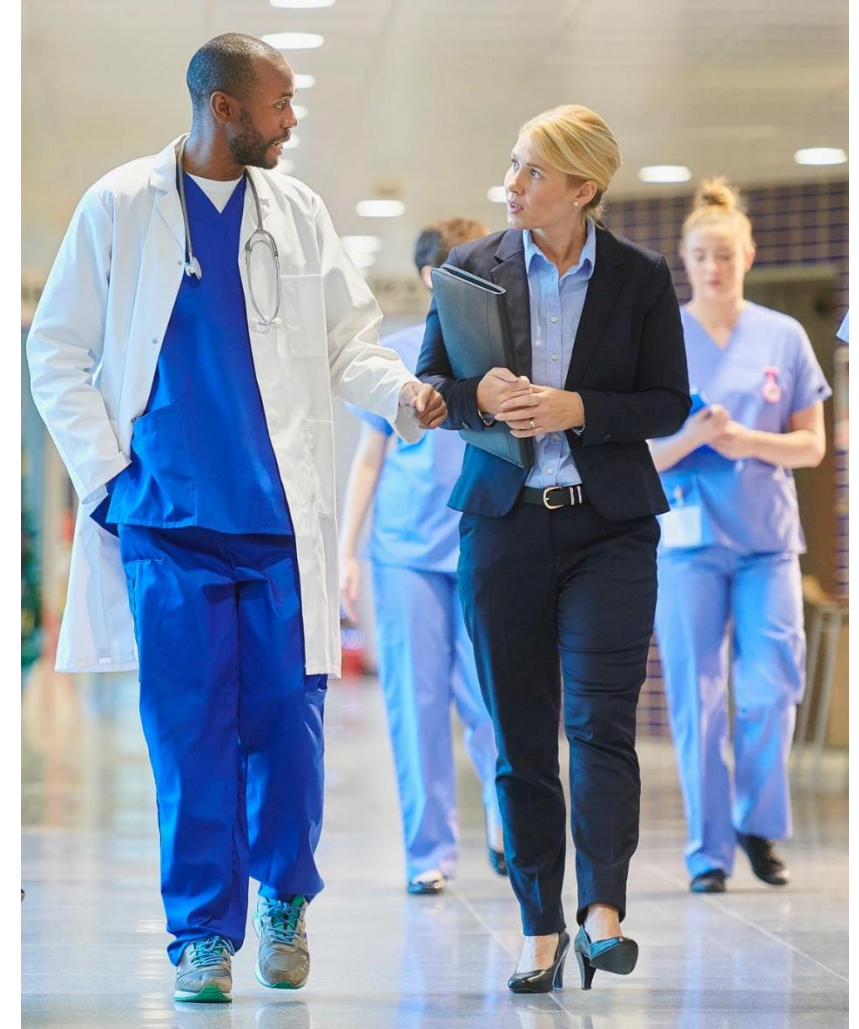
Group health plans must engage in all reasonable efforts **not** to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

Authorized releases are exempt so long as the parties comply with the terms of the authorization (i.e., authorization that allows a release to a specific vendor/provider)



New HIPAA Privacy Regulations – **Reproductive Health Rights**

- On April 22, 2024, HHS issued [updated HIPAA regulations](#) implementing new protections and restrictions on when information may be disclosed to a third party about individuals who provided or sought health reproductive services (including abortion).
 - These updates were enacted mostly in response to SCOTUS overturning *Roe v. Wade*, thereby granting the states the authority to regulate abortions.
- Implements protections against disclosing information to third parties related to reproductive services if the services are performed in a state where it is lawful.
- Establishes the use of an attestation prior to disclosing reproductive health information to a third party.
- Requires distribution of a new HIPAA Privacy Notice to covered participants no later than February 16, 2026.
- Extends HIPAA civil and criminal penalties for the violation of these new reproductive health care rights.



New HIPAA Privacy Regulations - **Reproductive Health Rights**

Regulated Parties:

All HIPAA Covered entities and their business associates.

- **Group health plans:** all self-insured, all level funded, and fully-insured that access PHI.
- Rules will apply mostly to medical plans, pharmacy plans, health FSAs, and HRAs as these plans may reimburse or pay for health reproductive services.

Effective dates:

- **June 26, 2024:** Amended rules officially go into effect
- **December 23, 2024:** HIPAA-covered group health plans become subject to the new rules and must:
 - Update HIPAA Policies and Procedures documents to account for the new protections granted to individuals seeking reproductive health services.
 - Implement new attestation requirements
 - Update HIPAA Business Associate Agreements to include new protections and use of attestations
 - Train staff on updated internal procedures to align with the new rules
- **February 16, 2026:** Update and distribute new HIPAA Privacy Notices that include the new protections around disclosing information regarding reproductive healthcare.

HHS Model Attestation Form for Use or Disclosure of PHI

Within the form, the PHI requester must select ONE of the two following boxes:

- The purpose of the use or disclosure of protected health information is not to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care or to identify any person for such purposes. - **Would apply for states that allow abortion**
- The purpose of the use or disclosure of protected health information is to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, or to identify any person for such purposes, but the reproductive health care at issue was not lawful under the circumstances in which it was provided. - **Would apply for states that prohibit abortion**

Link to the form: [Model Attestation Form](#)

Link to abortion law state map: [Abortion law state map: See where abortions are legal or banned | CNN](#) - Updated July 29, 2024

Model Attestation Regarding a Requested Use or Disclosure of Protected Health Information Potentially Related to Reproductive Health Care

The entire form must be completed for the attestation to be valid.

Name of person(s) or specific identification of the class of persons to receive the requested PHI. <i>e.g., name of investigator and/or agency making the request</i>
Name or other specific identification of the person or class of persons from whom you are requesting the use or disclosure. <i>e.g., name of covered entity or business associate that maintains the PHI and/or name of their workforce member who handles requests for PHI</i>
Description of specific PHI requested, including name(s) of individual(s), if practicable, or a description of the class of individuals, whose protected health information you are requesting. <i>e.g., visit summary for [name of individual] on [date]; list of individuals who obtained [name of prescription medication] between [date range]</i>

I attest that the use or disclosure of PHI that I am requesting is not for a purpose prohibited by the HIPAA Privacy Rule at 45 CFR 164.502(a)(5)(iii) because of one of the following (check one box):

- ☐ The purpose of the use or disclosure of protected health information is not to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care or to identify any person for such purposes.
- ☐ The purpose of the use or disclosure of protected health information is to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, or to identify any person for such purposes, but the reproductive health care at issue was not lawful under the circumstances in which it was provided.

I understand that I may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if I knowingly and in violation of HIPAA obtain individually identifiable health information relating to an individual or disclose individually identifiable health information to another person.

Signature of the person requesting the PHI

Date _____

If you have signed as a representative of the person requesting PHI, provide a description of your authority to act for that person.

New Confidentiality of Substance Use Disorder Records

Effective Date: April 16, 2024

Patient Consent

- Allows a single consent for all future uses and disclosures for treatment, payment, and health care operations.
- Allows covered entities and business associates that receive records under this consent to redisclose the records in accordance with the HIPAA regulations.¹

Other Uses and Disclosures

- Permits disclosure of records without patient consent to public health authorities, provided that the records disclosed are de-identified according to the standards established in the HIPAA Privacy Rule.
- Restricts the use of records and testimony in civil, criminal, administrative, and legislative proceedings against patients, absent patient consent or a court order.

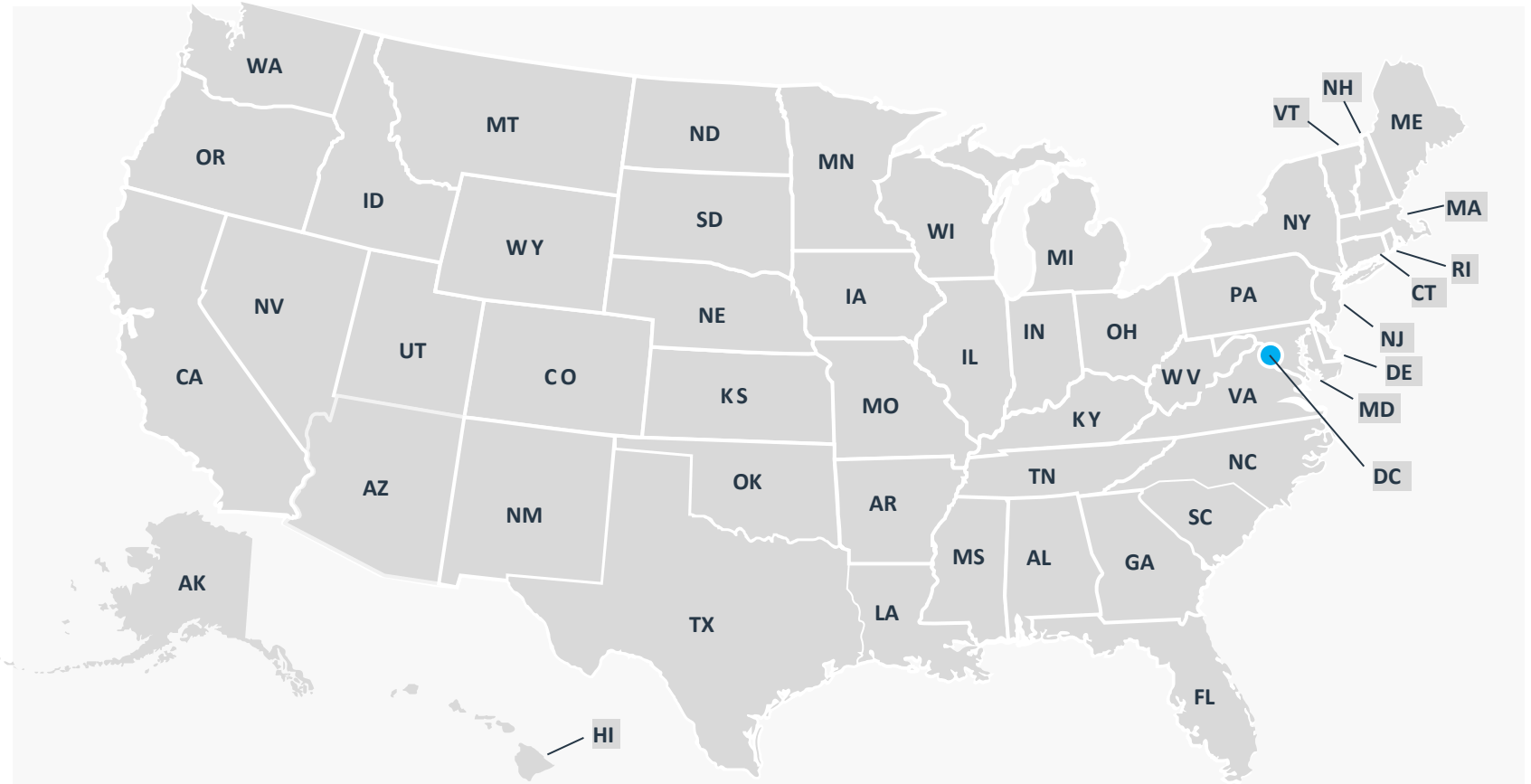
Penalties

- Aligns Part 2 penalties with HIPAA by replacing criminal penalties currently in Part 2 with civil and criminal enforcement authority that applies to HIPAA violations.

Privacy Standards and State Laws

HIPAA Privacy Standards do NOT override more strict state laws, which potentially requires health plans to support two systems and follow the more stringent state law.

For example, if a state requires that health plans keep their medical and claim records for 7 years before destroying them, but HIPAA requires 6 years, the health plan must follow the state law and keep their medical and claims records for 7 years.



What is Protected by the Security Rule?

- **Electronic** Protected Health Information (ePHI)
- EPHI is individually identifiable health information, relating to the past, present or future health condition of the individual, in electronic form when it is stored, maintained, or transmitted.
- Some examples of ePHI are:



Electronic claims

Email



Digital X-rays



Computer databases
with treatment history



Electronic medical
records (EMR)

HIPAA Security Standards

- HIPAA's security standards impose rules to protect confidentiality, integrity, and availability of electronic PHI.
- Covered entities must, among other things, perform a risk analysis and implement a risk management plan to protect electronic PHI from threats and vulnerabilities.

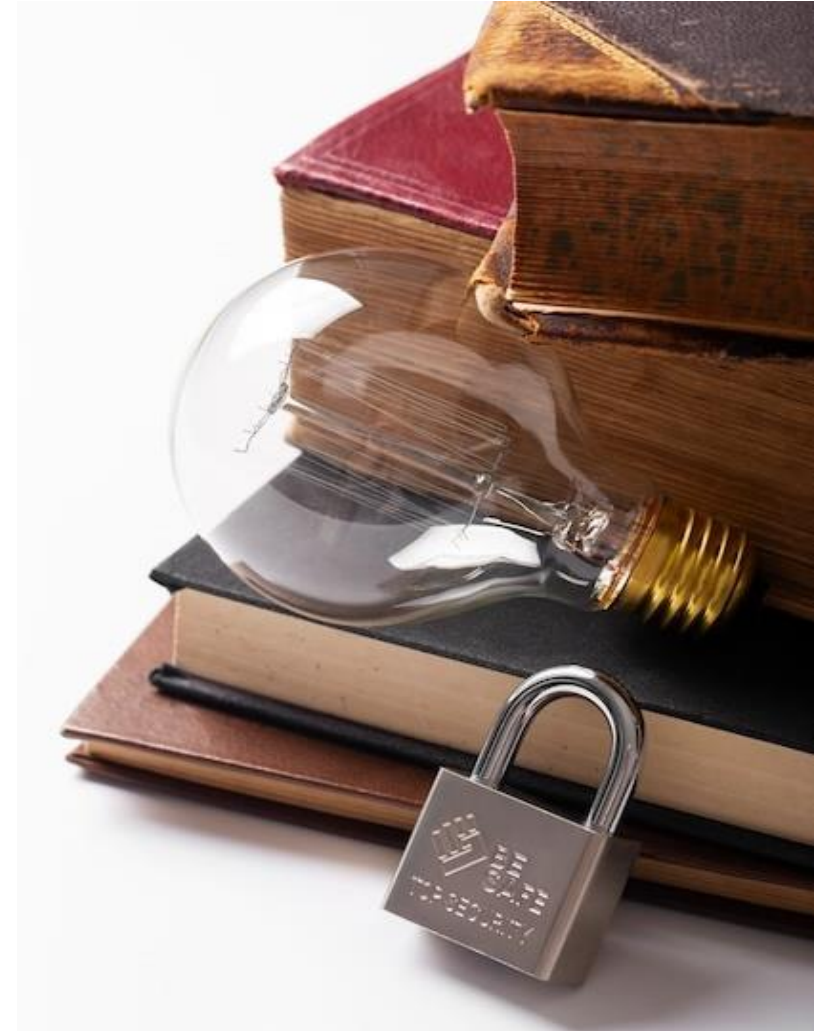
Who Must Comply:

- Any person or organization that stores or transmits individually identifiable health information electronically
- Includes both Covered Entities and Business Associates

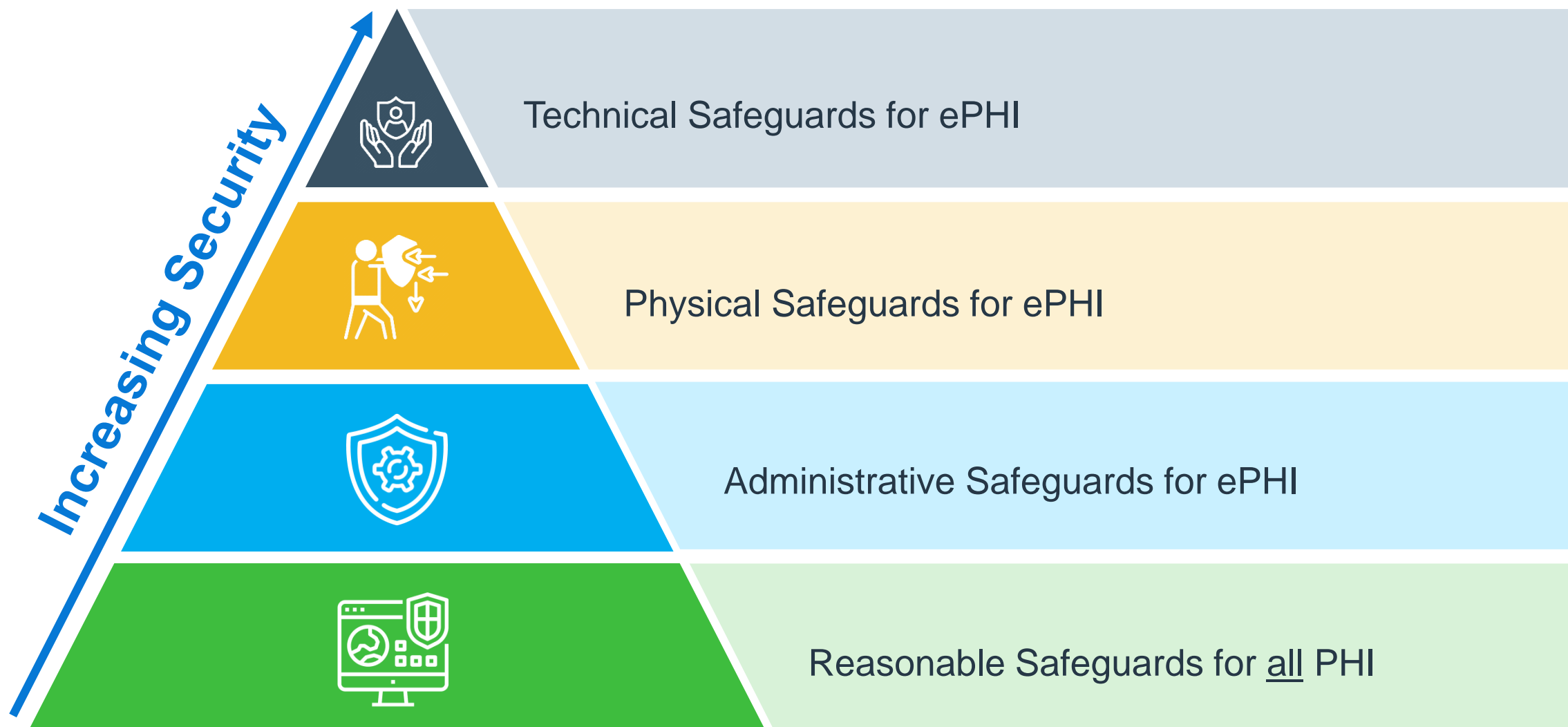


Overview of the Security Rule

1. Determine if your organization is subject to the HIPAA Security Rule
2. Appoint a HIPAA Security Officer
3. Have the HIPAA Security Officer and technical IT staff who will be helping implement HIPAA Security take a detailed HIPAA Security training course
4. Perform a risk assessment on your organization's environment
5. Develop a risk mitigation plan
6. Draft the necessary policies and procedures required by the Security standards to safeguard ePHI
7. Work with IT staff to implement security standards contained in the new policies and procedures
8. Train employees on new security policies and procedures and systems
9. Monitor compliance and perform periodic security systems evaluations (and take corrective actions as needed)



Security Rule Safeguards



Administrative Safeguards

Administrative Safeguards are administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the organization's workforce in relation to the protection of that information.

Standards of Administrative Safeguards

1. Security Management Process
2. Assigned Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security Awareness and Training
6. Security Incident Procedures
7. Contingency Plan
8. Evaluation
9. Business Associate Contracts

Administrative Safeguards Implementation

- Assigning a security officer
- Security awareness training
- Internal audits
- Contingency plans for emergencies
- Procedures for reporting security incidents

Compliance Obligations: Administrative Requirements

PHI Users must have the following:



Privacy officer must be designated and will be an individual to whom responsibility for privacy must be assigned



Contract with business associates must be in place (written contract assuring information will be safeguarded)



Forms and documents to support individual participant rights and to safeguard confidentiality of PHI



Policies, procedures and systems in place to protect PHI and individual rights



Ongoing training for staff and agents



Privacy complaint process and sanctions

Physical Safeguards

Physical measures, policies, and procedures to protect the organization's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Standards of Physical Safeguards

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

Physical Safeguards Implemented

- Computer servers in locked rooms
- Locked cabinets for records with PHI
- "Clean Desks"
- Data backups stored offsite
- Screen savers / screen locks
- Employee badges
- Shredding and disposal of PHI records
- Door locks
- Fireproof storage for records with PHI
- FAX Standard Cover Sheet (with confidentiality language)

Technical Safeguards

Technology and policy and procedures that protect ePHI and control access to it.

Standards of Technical Safeguards

1. Access Control
2. Audit Controls
3. Integrity
4. Person or Entity Authentication
5. Transmission Security

Technical Safeguards Implemented

- Usernames and passwords
- Security logs
- Access controls
- Firewalls
- Data encryption



Security Rule: Technology Neutral

Federally mandated “floor” of protection - primary objective to protect the confidentiality, integrity, and availability of individually identifiable health information in electronic form **when it is stored, maintained, or transmitted.**

The Security Rule is

1. A Federally Mandated “Floor” of Protection
2. Comprehensive
3. Scalable
4. Technology Neutral

Factors for Reasonable and Appropriate

- Size, complexity and capabilities
- Costs of security measures
- Their access to and use of ePHI
- Probability and criticality of potential risks to ePHI
- Technical infrastructure, hardware and software security capabilities

HIPAA HITECH Act



Summary of HITECH Act (HIPAA 2.0)

Enforcement and Penalties

- Enforcement provisions include penalties, a tiered penalty system, and an HHS mandate that it perform periodic compliance audits

Business Associates

- HIPAA *Privacy and Security requirements apply directly to Business Associates*
- Business Associates are included under the HIPAA enforcement umbrella and are subject to civil and criminal penalties for non-compliance
- Subcontractors are considered Business Associates
- Strict requirement for a Business Associate Contract to be in place

Breach Notification

- *Data breach notification requirements for unauthorized use and disclosure of “unsecured PHI”* as well as improper use or disclosure of PHI

Expanded Patient Rights

- *Individuals have the right* to request that *their PHI* for healthcare treatment or service *not be disclosed to a third-party health plan or payer if payment for the treatment or service is paid out of pocket and paid in full at the time of service.*

Electronic Health Records (EHRs)

- *Individuals have the right to obtain a copy of their electronic health records* or to have them forwarded to a third party
- *Accounting of disclosures definition* expanded to include EHRs
- Prohibition on the sale of PHI or EHRs
- Eligible healthcare professionals and hospitals can qualify for Medicare and Medicaid incentive payments when they adopt certified EHR technology and use it to achieve specified objectives

Marketing and Fundraising

- Rules regarding marketing/fundraising communications

Business Associates



Business Associate Contracts / Agreements (BAA)

01

Outlines Covered Entities and Business Associates duties

02

Business Associates must have an agreement in place with any of its subcontractors ("**downstream PHI**")

03

Covered Entities and Business Associates must receive “satisfactory assurances” (i.e. that their PHI will be protected as required by HIPAA)

Business Associate Legal Obligations

HIPAA Privacy

- PHI uses and disclosures not permitted under BAA
- Minimum necessary requirement
- Breach notification requirements
- Provide copy of PHI in electronic form
- Disclosure to HHS for investigations
- Accounting of disclosures
- BAA with subcontractors

HIPAA Security

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- BAA with subcontractors
- Policies and procedures
- Security official
- Risk analysis
- Workforce training

Response to Cyber Security Incidents

HHS's Office for Civil Rights (OCR) Quick-Response Checklist:

- Explains the steps for HIPAA-covered entities and business associates to take in response to a cyber-related security incident
- Affected Entities Must:
 - Execute response and mitigation procedures and contingency plans
 - Report the incident to law enforcement
 - Report threat indicators to information-sharing and analysis organizations (ISAOs)
 - Follow the HITECH Act's breach notification requirements



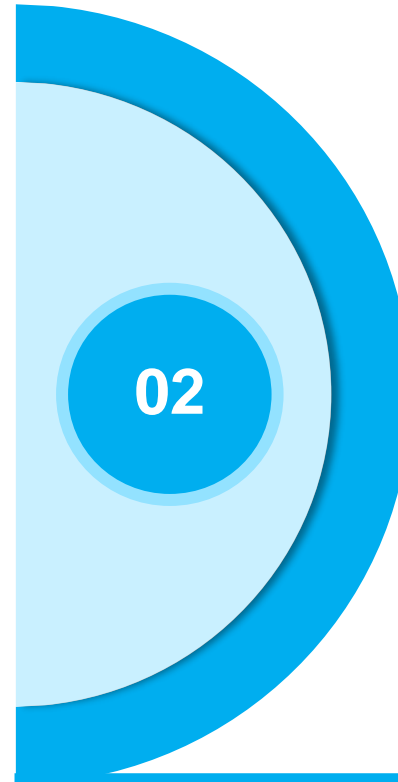
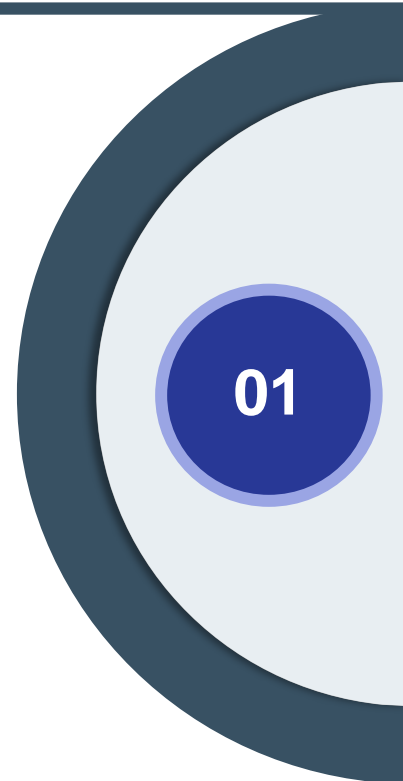
What is a Data Breach?

Definition of Breach (45 C.F.R. 164.402)



Impermissible use or disclosure of (unsecured) PHI

Rule presumes breach occurred unless the covered entity or business associate, demonstrates a low probability that the PHI has been compromised based on a risk assessment.



Unsecured PHI

“Unsecured protected health information” means protected health information (PHI) that is usable, readable, or decipherable to unauthorized persons through use of a technology or methodology.



Breach Discovery

A breach is treated as discovered:

- On first day the breach is known to the covered entity -OR-
- In the exercise of reasonable diligence, it ***should have been known*** to the covered entity

Breach notification period clock starts when the organization knew or should have known that a breach occurred



Assessing a Data Breach

Four-factor risk assessment

1. Nature and extent of PHI involved (including identifiers) - can PHI be used in a manner adverse to the individual or their interests?
2. Identity of unauthorized user or recipient
3. Whether PHI was actually acquired or viewed (e.g., stolen laptop not accessed)
4. Extent to which risk has been mitigated (e.g., recipient signs confidentiality statement)

Burden on covered entity or business associate to prove and document low probability that PHI was compromised if no notification is made.

Example: *No breach notification required for an unauthorized disclosure if the disclosed PHI was encrypted in accordance with the guidance*



Security Breach Notification

Notify each affected individual by first-class mail or email (upon approval of this method) including:

- Circumstances of the breach
- Date of the breach
- Date of the discovery
- Type of PHI involved
- Steps individuals should take to protect themselves
- Steps the covered entity is taking to mitigate harm and to protect against any future breaches
- NOTE: Public posting of the breach is required where recipient contact information is not available and the breach affects 10+ individuals (post for 90 days)

Notice must be provided “without unreasonable delay” but no later than 60 days from discovery

Burden on covered entity or business associate to prove all required notifications given – or were not required

Security Breach Notification Report & Publication

Breach involving 500 or more individuals:

- Submit a report to the Secretary of HHS immediately
- Complete a public posting on the Health and Human Services (HHS) website
- Alert local media if those affected reside in the same area
 - Media outlets will make the decision whether to cover, after covered entity or business associate sends press release to the media outlets

Breaches involving fewer than 500 individuals:

- Maintain a log of such breaches and annually submit to HHS
- Vendor must notify federal trade commission of breaches caused by their products or services
- ***Business associates must notify covered entity***
- Mitigation required, to the extent possible, to reduce or eliminate harm caused by the breach

Breaches that Made Headlines

\$2.3 Million

Medical facility failed to take appropriate security measures and had patient records accessed by hacker as well as disclosing PHI to 3rd Party Vendors without BAA

\$4.8 Million

Hospital error where health records of 6,800 patients ended up online and searchable

\$100,000

Company that moved and stored medical records allowed 2,150 paper records unsecured outside the shredding facility

\$250,000

Health insurance provider had unencrypted laptop containing ePHI of 148 individuals stolen from an employee's auto

Key Takeaways

- Understand whether your plan has access to PHI
- Where applicable, have policies and procedures in place, and name Privacy/Security Officers
- Recognize that HIPAA compliance requires an ongoing commitment
- Your GHP HIPAA compliance obligations increase with your degree of self-administration or “hands on” PHI handling, regardless of plan funding
- The HIPAA Security Rule allows for scalability under “Reasonable and Appropriate” considerations but does not excuse employers of any size from maintaining adequate security measures
- HIPAA compliance is *no longer a contractual requirement* (if that) for business associates and subcontractors, it is a *strict requirement* under the HITECH Act
- Covered Entities and Business Associates must establish their own internal policies and procedures to address the new breach notification rules, deadlines, possible exceptions to those rules, and ongoing employee training



Thank you

For more information and resources, visit:
www.hubinternational.com

