MARSH & McLENNAN AGENCY

COUNT ON US!

2020 Employee Benefits Webinar Series

HIPAA Privacy and Security

Andie Schieler, J.D.
Compliance Center of Excellence, Compliance Consultant

March 19, 2020

WORLD CLASS. LOCAL TOUCH.

Agenda

1. Housekeeping
2. Some Basics
3. Uses and Disclosures of PHI
4. Breaches
5. Participant Rights
6. Enforcement and Penalties
7. Questions?

Housekeeping

Welcome

This presentation is intended to help you understand how and why some basic concepts under HIPAA's Administrative Simplification Rules and how you may be affected.

HIPAA's Administrative Simplification Rules include what are commonly referred to as the HIPAA Privacy and HIPAA Security Rules and are administered by the U.S. Department of Health & Human Services (HHS).

This presentation will focus on HIPAA as it relates to employer-sponsored benefit plans.

What is HIPAA?

HIPAA protects health information created or received by the employer's health plans by:

- Creating individual rights regarding "protected health information" or "PHI"
- Restricting the use and disclosure of PHI

HIPAA is primarily intended to:

(1) stop employers from making employment-based decisions based on information obtained through a health plan; and

(2) restrict the ability of employers and third parties to buy or sell an individual's health information

Other than HIPAA…

Just because HIPAA may not apply to a particular situation does not mean other laws do not:

- Americans with Disabilities Act – Limits employer inquiries into disabling/potentially disabling conditions;
- State data privacy laws – States laws may govern PDI or PII (e.g. California, Massachusetts, Texas);
- Genetic Information Nondiscrimination Act (GINA);
- Gramm-Leach-Bliley Act – Data privacy for financial institutions; or
- Your company's own data privacy policies

Some Basics

Protected Health Information

Protected Health Information (PHI)

- Information about: (i) a past, present, or future health condition, (ii) treatment for a health condition, or (iii) payment for the treatment of a health condition
- Identifiable to a specific individual
- Created and/or received by a Covered Entity or Business Associate acting on behalf of a Covered Entity
- Maintained or transmitted in any form

Does not include employment records held in the capacity of an employer (but other laws may apply)

PHI Identifiers

- Names
- Addresses
- Zip Codes
- Dates (except year)
  - DOB
  - Admission date
  - Discharge date
  - Treatment date
- Telephone #s
- Fax #s
- Email Addresses
- SSNs
- IP addresses
- Fingerprints
- Full face photos
- Medical record #s
- Account #s
- Certificate / License #
- Vehicle ID (plates, VINs)

Some health information is automatically identifiable even if none of these identifiers are present.

Covered Entities

1. **Health care providers who conduct certain standard electronic transactions**
2. **Health plans**
   a) Self-insured – The plan is generally subject to all of the HIPAA compliance obligations
   b) Fully Insured – The HIPAA compliance obligations generally belong to the insurance carrier if the plan sponsor is “hands off” PHI
3. **Health care clearinghouses**

Fully Insured Health Plans

If the only PHI received by the plan from an insurance carrier is summary health information or enrollment information, then the plan only has to comply with:

- Non-intimidation / non-retaliation requirement
- Non-waiver of rights requirement

Hybrid Entity

If a plan provides health benefits and non-health benefits, the plan must comply with HIPAA with respect to the health benefits

- For example, a wrap plan that incorporates medical, dental, and vision benefits is a hybrid entity if it also incorporates life, AD&D, and disability

Records for the health benefits must be separate from non-health benefits

- PHI cannot be used by non-health benefits without an authorization

Who Needs Training?

Covered Entity workforce must be trained as necessary and appropriate for members to carry out their work functions

- The plan's Privacy, Security & Complaint Officer(s)
- Any other employee with access to PHI as a regular part of their job function such as the benefits department (frequency of access does not matter)
  - Ask: Is the access a regular part of my job function, or was it merely incidental?

Others benefit from understanding why they can't or shouldn't receive certain information

Group Health Plans

Yes	No	Maybe So
Medical	AD&D, STD, LTD	Onsite Clinics
Prescription Drugs	Business Travel Accident	Long-Term Care
Dental	Leave Administration	Wellness Programs
Vision	Life Insurance	
Health FSAs	**Health Savings Accounts***	
HRAs	Dependent Care FSAs / DCAPs	
EAPs (more than referral service)	Stop-Loss	
	Workers' Compensation Insurance	

***This tends to surprise people, but HSAs are generally individually owned accounts and not employer-sponsored group health plans.

A plan is exempt if it covers fewer than 50 current and/or former employees and is self-administered by the employer without assistance from a third party.

Business Associates

- A third party that requires PHI to perform some function or service on behalf of a group health plan
- The third party might create, receive, store, or transmit the PHI in this role, but it must be “PHI sticky” in at least one of those ways to be considered a Business Associate
- Many of HIPAA’s Privacy and Security requirements apply directly to Business Associates

Examples of Business Associates

Yes	No	Maybe So
Third party administrator (TPA)	Plan sponsor/employer	External legal counsel
Pharmacy benefit manager	Stop-loss carrier	Accountants if PHI will be disclosed in connection with an audit or review
COBRA administrator		
Broker/consulting firm		
Actuaries		
Storage companies that store paper copies of e-PHI		
Cloud service providers		

Really? Stop-Loss isn't a Business Associate?

Is a reinsurer a business associate of a health plan?

Answer: Generally, no. A reinsurer does not become a business associate of a health plan simply by selling a reinsurance policy to a health plan and paying claims under the reinsurance policy. Each entity is acting on its own behalf when the health plan purchases the reinsurance benefits, and when the health plan submits a claim to a reinsurer and the reinsurer pays the claim. However, a business associate relationship could arise if the reinsurer is performing a function on behalf of, or providing services to, the health plan that do not directly relate to the provision of the reinsurance benefits.

Source: HHS FAQ

Note: Stop-loss is usually purchased by the employer and not the plan. If HHS feels that a stop-loss carrier is not a business associate when the policy is purchased by the plan, the argument that it also isn't a business associate when purchased by the employer is very compelling. A confidentiality or non-disclosure agreement is still a good idea.

Business Associate Agreement (BAA)

- BAA is a contract between a Covered Entity and a Business Associate
- Must be in writing and contain certain provisions:
  - Addresses the reason(s) PHI may be used or disclosed by Business Associate
  - Addresses the parties' obligations and responsibilities under HIPAA
  - The parties may incorporate other contractual provisions provided they do not conflict with HIPAA
- BAA may also shift burden of providing breach notices to participants
- Sample provided on HHS website

Uses and Disclosures of PHI

Core Principles

- Limit uses and disclosures of PHI to authorized purposes
- Disclose or request only the minimum necessary information to accomplish the objective
- Know the authorized parties who can access or receive PHI
- Establish safeguards to prevent and minimize incidental disclosures

Uses and Disclosures of PHI

Plans cannot disclose PHI, unless:

- Required by the regulations
- Permitted by the regulations
- Authorized by the individual

Disclosure to Employer/Plan Sponsor

Plan can disclose PHI to Employer:

- To carry out certain plan administration functions if:
  - Plan documents include necessary HIPAA language, and
  - Notice of privacy practices states this is a permitted disclosure

In most cases, only members of the Covered Entity workforce can access or receive PHI to perform plan administrative functions

- Summary health information so employer can obtain premium bids or amend the plan
- Enrollment information from a plan

Enrollment information from an employer's HRIS system or similar record is an employer record and is not PHI.

Required Uses and Disclosures

1. **Disclosures to comply with an individual's:**

    a) right to access

    b) right to accounting

2. **Disclosures to HHS in connection with an investigation**

Permitted Uses and Disclosures

No authorization is required for the following uses and disclosures:

- To the individual himself/herself
- Within the Covered Entity
- For treatment, payment and healthcare operations
  - Enrollment and/or eligibility processing, claims analysis, underwriting, plan design, etc.
  - M&A due diligence
- To family/friends (with opportunity to object)
- For certain public policy activities (see next slide)

Permitted Public Policy Activities

- Abuse, Neglect or Domestic Violence
- Health Oversight Activities
- Judicial and Administrative Proceedings
- Law Enforcement
- Coroners, Medical Examiners, Funeral Directors
- Organ Donation
- Serious Threat to Health or Safety
- Compliance with Workers' Compensation Laws
- Immunization Records of Students

Contents of Valid Authorization

Must be signed and specifically describe:

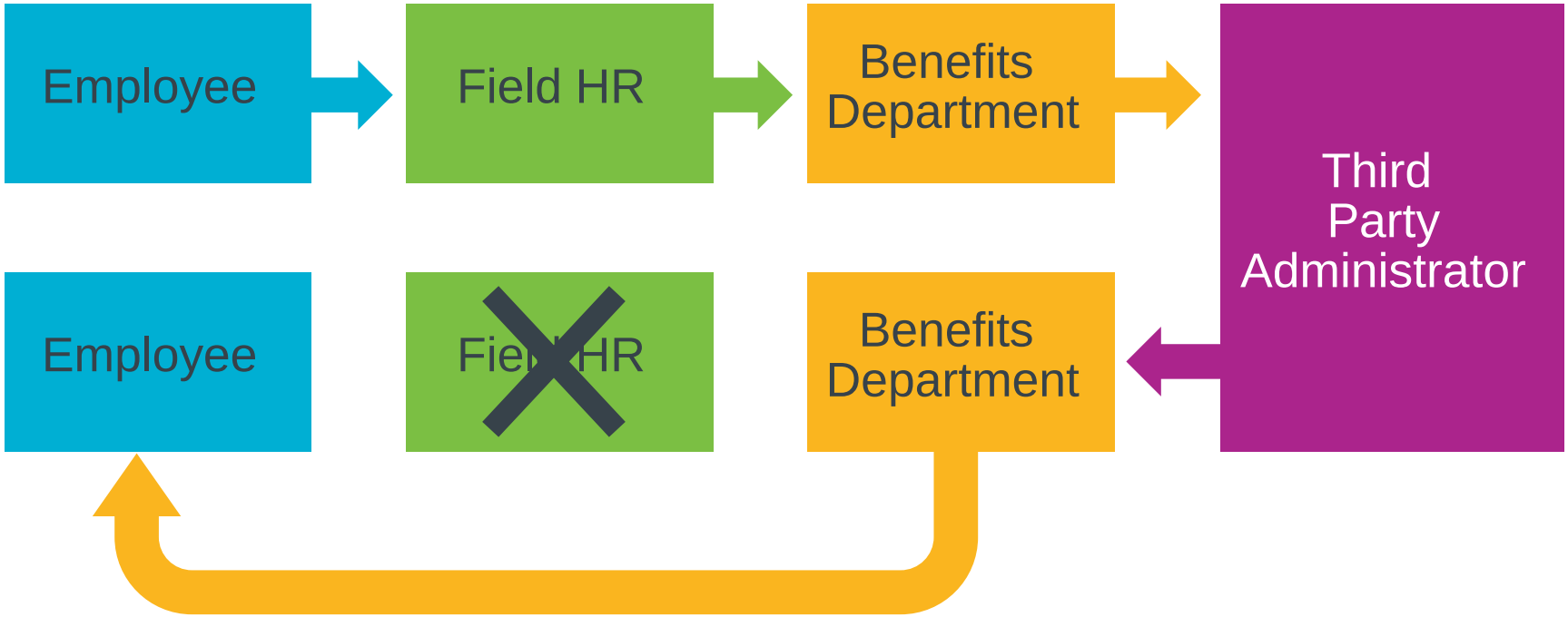
- Information that will be used/disclosed
- Individuals disclosing information
- Individuals receiving information
- Expiration date
- Individual’s right to revoke authorization at any time
- Procedure for revocation

Minimum Necessary Standard

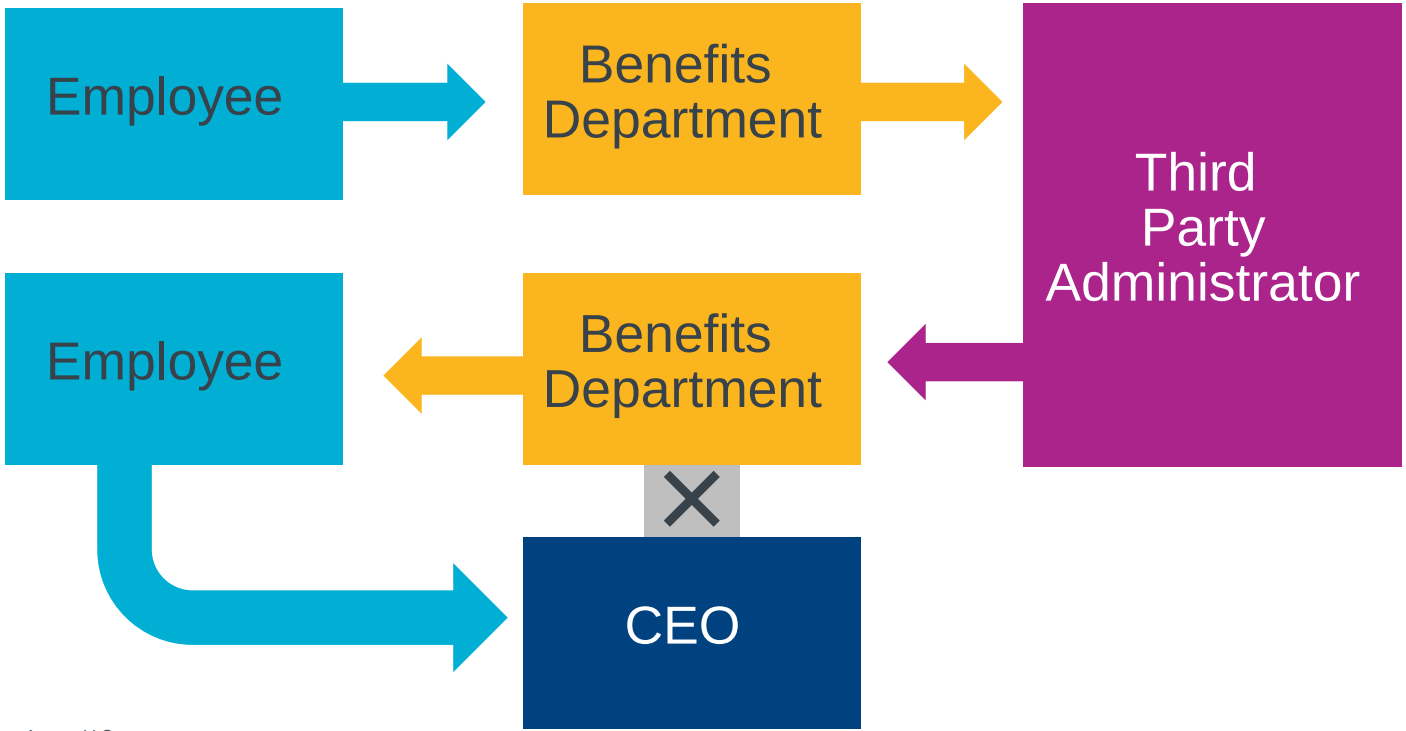
Must make “reasonable efforts” to use, disclose, and request only the minimum amount of PHI needed.

- Develop and implement policies to reasonably limit uses and disclosures to minimum necessary
- “Do I need this information to do my job?”

HR Advocacy Model



HR Advocacy Model



Overview of Security Rule

- Created standard protocol for transmitting and storing PHI and electronic PHI
- 5 categories of safeguards in regulations, each with standards and implementation specifics:
  - Administrative
  - Physical
  - Technical
  - Organizational
  - Documentation
- Covered Entities must comply with all safeguards
- Business Associates must comply with administrative, technical and physical

You must document the plan's processes and procedures!

Reasonable Safeguards

- Keep PHI in a secure location
  - Locking file cabinets with limited access to keys
- Private discussions involving PHI
- Pick up print jobs immediately
- Log off computers
- Computer monitor filters or positioning

Reasonable Safeguards

- Shred old documents
- Password protection of documents containing PHI
- Limited access to your electronic system
- Encryption of emails containing PHI

Breaches

Breach of PHI

A breach is the impermissible acquisition, access, use or disclosure of unsecured PHI that violates the HIPAA Privacy Rule

- Presume a breach has occurred unless there is a low probability that PHI has been compromised, based on:
  1. What and how much PHI was involved and how likely is it that a specific individual can be identified?
  2. Who got it?
  3. Was the PHI was actually acquired or viewed?
  4. What steps were taken to mitigate the risk of harm?

Secured versus Unsecured PHI

Two methods for securing PHI

1. “Destruction” of paper or electronic media beyond the ability to read or reconstruct the PHI
2. “Encryption” using one or more processes requiring an encryption key specified in regulations (always electronic PHI)

All other PHI is generally considered unsecured

Note: A breach doesn’t occur if the unsecured PHI was accessed by or disclosed to an authorized party, although the access or disclosure may still present a lesser issue.

Exceptions

- Unintentional, good-faith access or use of PHI by person acting on behalf of Covered Entity or Business Associate within the scope of their duties
- Inadvertent disclosure of PHI to authorized person within Covered Entity or Business Associate
- Good-faith belief the unauthorized person cannot reasonably use or retain the PHI

Burden of proving exception falls on person claiming it!

Breach Notification

If you know PHI has been accessed, used or disclosed and it should not have been, notify the Privacy Officer IMMEDIATELY.

- Breach notification requirement is 60 days from the date Covered Entity knows (or should have known) of the breach, which may be from date notified by Business Associate
- HHS indicates 60 days may be unreasonable under certain circumstances

Breach Notification

- Notification must include:
  - A brief description of what occurred, including the date of breach and date of discovery
  - A description of the type of PHI involved
  - Steps affected individuals should take to protect themselves
  - What the covered entity is doing to mitigate the harm
  - Contact information for covered entity
- Provide the notice via first-class mail to last known address (may also post on intranet)
- Use telephone if risk of harm is imminent

Breach Notification

Fewer than 500 individuals affected

- Notify individuals within 60 days of discovery
- Notify HHS within 60 days of the end of the calendar year of discovery
- Maintain information for six years

500 or more individuals affected

- Notify individuals within 60 days of discovery
- Notify HHS within 60 days of discovery
- Notify prominent media outlets if 500 or more affected in single state or jurisdiction (media is not required to publish)
- Maintain information for six years

Notice to HHS provided here: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf

Large breach “scarlet letter” page: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Participant Rights

Participant Rights

- Right to privacy as mandated through HIPAA regulations
- Right to access and copy their health information
- Right to amend their personal health records
- Right to know “who else” has received their health information
- Right to request restrictions on family members who may access their health information
- Right to request restrictions on the use of their PHI

The employer has a right to deny unreasonable requests.

Participant Rights

- Right to request that health information be communicated to them in a confidential manner
- Right to receive a paper version of the Notice of Privacy Practices (NPP)

Note: Prevailing thought that a Covered Entity can only make the permissive PHI disclosures that are described in the NPP (Example: For research purposes). It is definitely a good idea to make sure your notice is comprehensive!

- Right to make a formal complaint if they feel their PHI has been disclosed inappropriately

Enforcement and Penalties

Civil Enforcement

- HHS may audit based on complaints or on own initiative
- State attorneys general can bring civil actions against health plans and get damages on behalf of state residents
- Employers need policies/procedures on sanctions for violations

Civil Penalties

No knowledge violated HIPAA

- Minimum civil penalty of $100 per violation

Reasonable cause

- Minimum civil penalty of $1,000 per violation

Willful neglect

- Minimum civil penalty of $10,000 per violation
- $50,000 per violation if not corrected

Criminal Penalties

- Criminal actions can be brought against any individual, not just the plan, who wrongfully discloses PHI
- Many criminal penalties assessed by HHS are for failures to cooperate with an investigation
- Maximum $250,000 in fines and up to 10 years in prison

Questions

MarshMMA.com