MARSH & McLENNAN AGENCY

WORLD CLASS. LOCAL TOUCH.

# HIPAA TRAINING MODULE

# Agenda

- HIPAA  OVERVIEW
- HIPAA  REQUIREMENTS
- EXAMPLES
- QUIZ TIME

# HIPAA OVERVIEW

Knock Knock!
-Who's there?
HIPAA!
-HIPAA who?

I can't tell you that.

someecards
user card

# HIPAA Overview

**H**EALTH

**I**NSURANCE

**P**ORTABILITY &

**A**CCOUNTABILITY

**A**CT

**H**EALTH

**I**NFORMATION

**T**ECHNOLOGY FOR

**E**CONOMIC &

**C**LINICAL

**H**EALTH

**A**CT

# HIPAA / HITECH Regulations

## GINA (2008)

- No use or disclosure of genetic information for underwriting

## HITECH (2009)

- Breach notification
- Business Associate (BA) obligations
- Stricter penalties for breaches
- Random periodic audits

## HITECH FINAL REGULATIONS (2013)

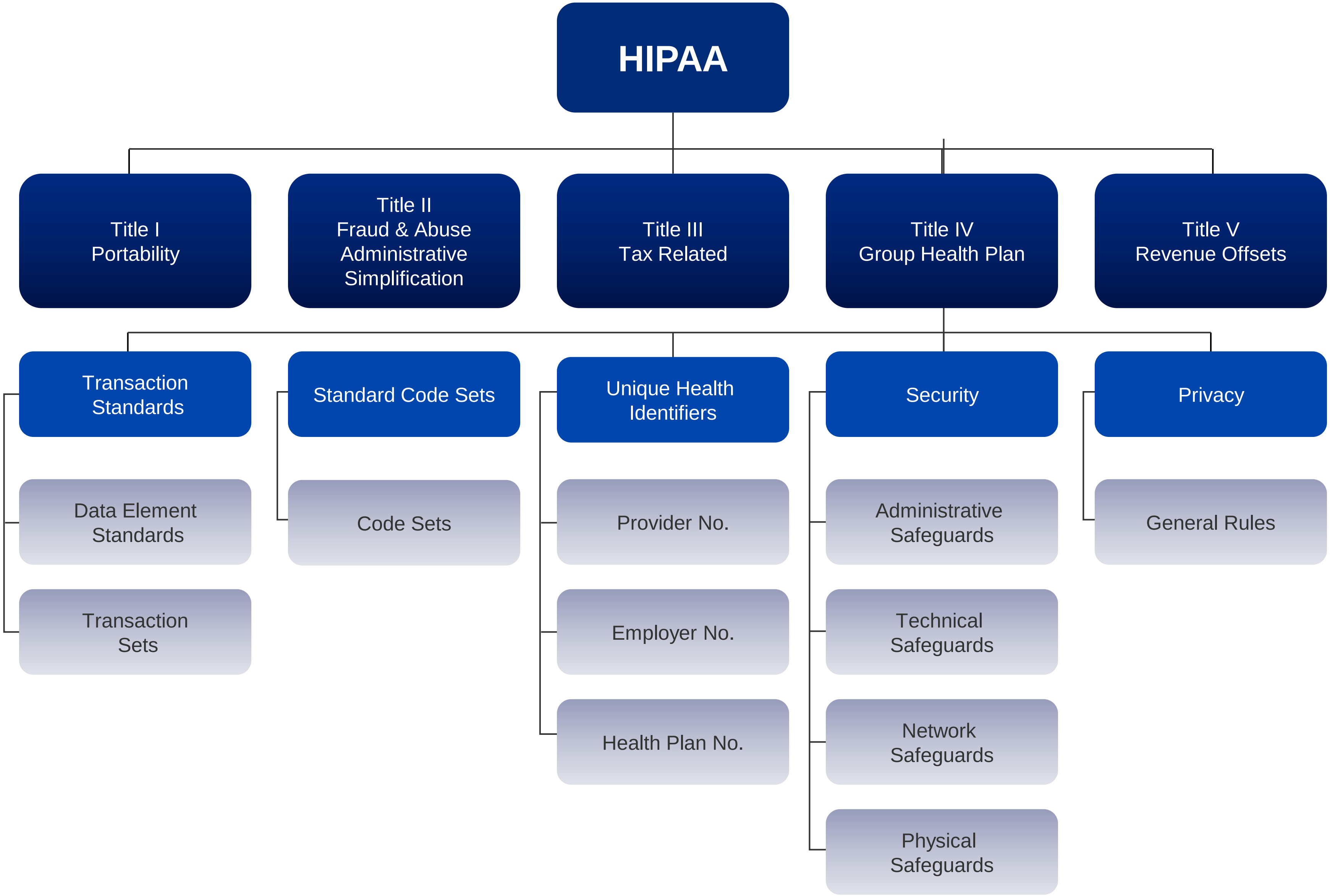
- Subcontractors of Business Associates have similar obligations as BAs
- Stricter “breach” definition

# Covered Entities: Who must comply with HIPAA?

## COVERED ENTITIES:

- Health Care Providers
- **Health Plans**
- Health Care Clearinghouses

*Note: Business Associates are* ***not*** *a Covered Entity, but are still subject to the requirements under the HIPAA Privacy & Security Rules effective February 17, 2010)*

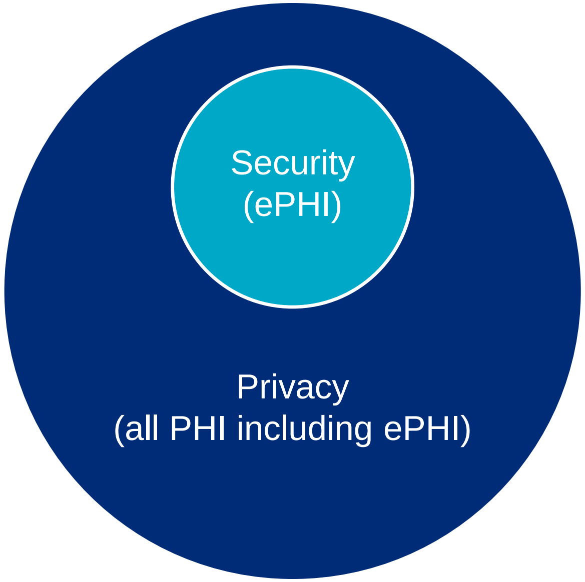


HIPAA
Title I
Portability
Title II
Fraud & Abuse
Administrative
Simplification
Title III
Tax Related
Title IV
Group Health Plan
Title V
Revenue Offsets
Transaction Standards
Data Element Standards
Transaction Sets
Standard Code Sets
Code Sets
Unique Health Identifiers
Provider No.
Employer No.
Health Plan No.
Security
Administrative Safeguards
Technical Safeguards
Network Safeguards
Physical Safeguards
Privacy
General Rules

# HIPAA Privacy vs. HIPAA Security

## PRIVACY

- Paper-based PHI
- Orally-communicated
- Rights of individual



Security
(ePHI)

Privacy
(all PHI including ePHI)

## SECURITY

- Complements HIPAA privacy
- Restricts access and use of ePHI
- Protects ePHI

# What is HIPAA?

- Maintains the confidentiality and data integrity of PHI (regardless of form):
  - **Verbal discussions** (i.e., in person or on the phone)
  - **Written communication** (i.e., emails, faxes, copies, EOBs, 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 or disclosure of Protected Health Information (PHI)
  - **Use** – when reviewing or discussing PHI internally (audits, training, customer service, quality control)
  - **Disclosure** – when we release or provide some one else's PHI to a third-party without the presence of the person who owns the PHI (i.e., carriers, employers, etc.)
- Provides security standards
- Provides for healthcare portability
- Provides for privacy rights
- Structures how carriers, employer groups and others handle PHI
- Structures how employer groups receive and use PHI

# Protected Health Information (PHI)

## PROTECTED HEALTH INFORMATION

- Created or received by a covered entity
- Related to an individual’s past, present, or future health or condition
- That identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual
- **May excludes information included in education records, employment records and regarding a person deceased for more than 50 years**

NOTE: HEALTH INFORMATION MAINTAINED AS PART OF EMPLOYMENT RECORD IS EXEMPT… BUT OTHER STATE PRIVACY LAWS MAY APPLY!

# Personal Identifiers

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification numbers
- Vehicle Identifiers/Serial numbers/License plate numbers
- Internet protocol addresses
- Health plan numbers
- Full face photographic images and any comparable images
- Web universal resource locaters (URLs)
- Any dates related to any individual (date of birth)
- Telephone numbers
- Fax numbers
- Email addresses
- Biometric identifiers including finger and voice prints
- Any other unique identifying number, characteristic or code

MARSH & McLENNAN AGENCY

WORLD CLASS. LOCAL TOUCH.

# HIPAA PRIVACY REQUIREMENTS

# HIPAA Privacy Requirements

## RESTRICT USE AND DISCLOSURE OF PHI

- Minimum Necessary Standard
- Authorizations are necessary for any release of PHI, except in the following instances:
  - Payment, Treatment or Operations (PTO)
  - Summary Health Information
  - As required by law
  - Public health

## INDIVIDUAL RIGHTS

- Restrictions
- Access
- Accounting
- Amendment

## BUSINESS ASSOCIATES

- Business Associate Agreements
- Subcontractor’s of BAs - duties

# Minimum Necessary Standard

**WHEN USING, RECEIVING, OR DISCLOSING PHI, ASK YOURSELF:**

- Do I need to know this information?
- Is it necessary for my job?
- How much do I need to know?
- How much do other people need to know?
- Can anyone overhear my conversation?

*Note: The key is to balance the right to privacy against the need for information*

# Authorization Forms

### WHEN AUTHORIZATION IS REQUIRED

- Use or disclosure of psychotherapy notes
- An Authorization is needed for the use and disclosure of PHI for marketing purposes
- When selling PHI
- When helping employees with claims issues where you must share with a third-party an employee’s PHI

### WHEN AUTHORIZATION IS NOT REQUIRED

- Disclosures to the individual to whom the PHI belongs to
- Uses and disclosures for treatment by your physician
- Uses and disclosures for quality assurance activities
- When assisting employees with claims or leave issues, and do not share their PHI with a third-party

# Business Associates

## BUSINESS ASSOCIATES

- An entity that is designated by a Covered Entity to handle/receive/disclose/use its PHI in the Administration of its duties as the Covered Entity.  Examples include:
  - Third Party Administrator in a Self-Funded Plan
  - Broker
  - Storage facility for PHI
  - Shredding company
  - A Pharmacy Benefits Manager that manages a health plan’s pharmacist network

# HIPAA SECURITY REQUIREMENTS

# HIPAA Security Requirements

## ADMINISTRATIVE PROCEDURES

- Documented disaster recovery plan
- Documented policy & training
- Limited access
- Secure storage
- Discuss PHI in private using minimum necessary standard

## PHYSICAL SAFEGUARDS

- Workstations are in secure area & logged off
- Use email password protected attachments
- Save in restricted drawer or file
- Guests / visitors escorted

## TECHNICAL SECURITY SERVICES

- Secure access with passwords
- Secure data (i.e., read only, read & write, read, write & change authority)
- Transmit securely

## TECHNICAL SECURITY MECHANISMS

- Firewalls
- Encryption
- Limit access via IT authorized user profiles

# Implementing Safeguards

## ASSESS AREAS OF RISK USING PHI FLOWCHART

- Map where PHI comes in
- What happens to it while it is being used/stored/disclosed
- Where it goes after use

## IDENTIFY WHAT IS PHI YOU MAY COME ACROSS

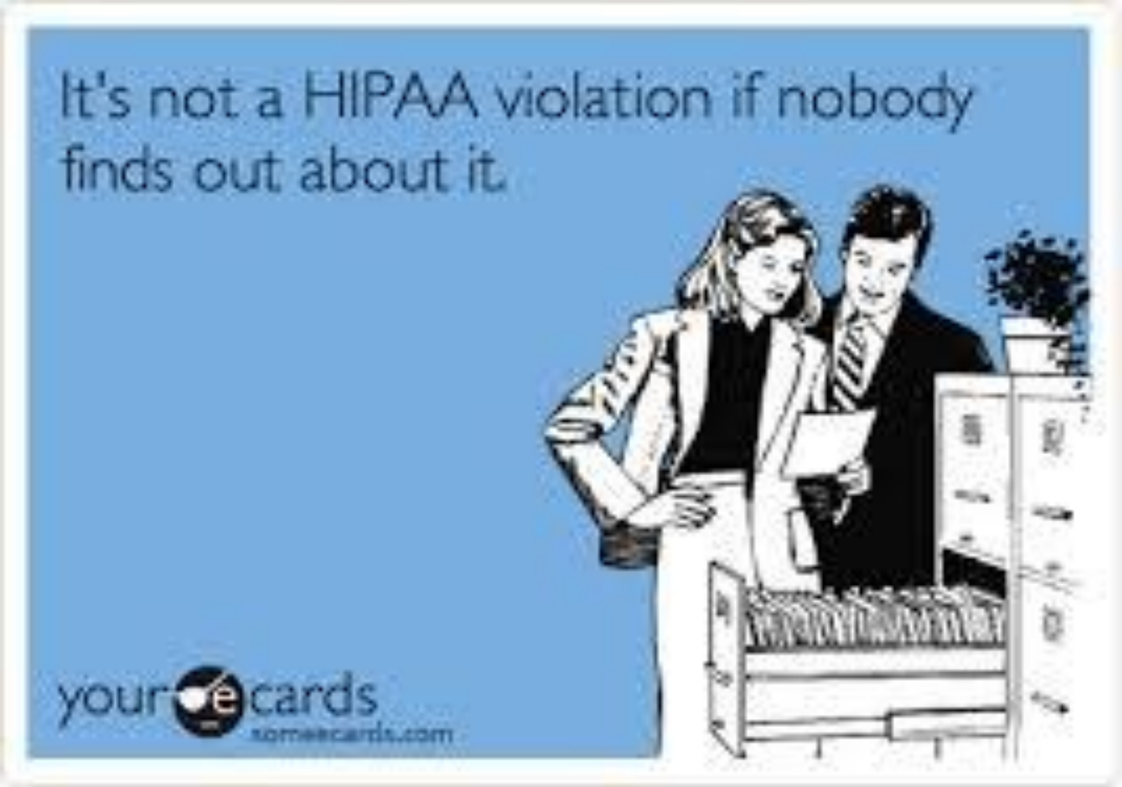
- EOB
- Claims
- Sick notes??
- Leave certifications??

## IDENTIFY AREAS OF RISK AND IMPLEMENT SAFEGUARDS TO PROTECT PHI FROM INTENTIONAL AND UNINTENTIONAL USE AND DISCLOSURE

- Limit access
- Firewalls
- Prevent overhearing when discussing PHI

© Mike Baldwin / Cornered

"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."



It's not a HIPAA violation if nobody finds out about it.

# Security Breach

## DEFINITION OF BREACH (45 C.F.R. 164.402)

Impermissible use or disclosure of unsecured PHI is assumed to be a breach 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 not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology required by the Breach Notification Rule

# Security Breach

## PRESUMPTION OF BREACH

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

# Security Breach

## HIPAA REQUIRED NOTIFICATION FOR “BREACHES” OF “UNSECURED PHI”

- “Breach” is the unauthorized acquisition, access to, use or disclosure of PHI (including improper disposal) which “**compromise the security or privacy of PHI”**
- Unsecured PHI can be in any form
- If no PHI, no breach (e.g., de-identified information and employment records)
- If PHI is secured, there is no notification requirement

## TWO METHODS OF SECURING PHI:

- Encryption
- Destruction

# Examples of Breaches

- Fax document to wrong location
- Telling your friends in the office about John Smith’s amputation
- Putting PHI in the trash instead of a secure shred bin
- Enter incorrect medical record number
- Reply all to an email where the email contains PHI
- Taking PHI out of the office
- Forgetting to verify identity
- *What other types of breaches can you think of?*

# Security Breach Notification

Notify each affected individual by first-class mail or email (upon approval of this method), and include the following information:

- 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
- Public posting required where contact information is not available and breach affects 10+ individuals (post for 90 days)

Notice must be provided “without unreasonable delay”; but no later than 60 days from **discovery** of the breach

BURDEN ON THE COVERED ENTITY OR BUSINESS ASSOCIATE TO PROVE AND DOCUMENT LOW PROBABILITY THAT PHI WAS COMPROMISED IF NO NOTIFICATION IS MADE

# Security 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

Notification time period for a breach begins when the organization did or should have known it existed

# Security Breach Notification

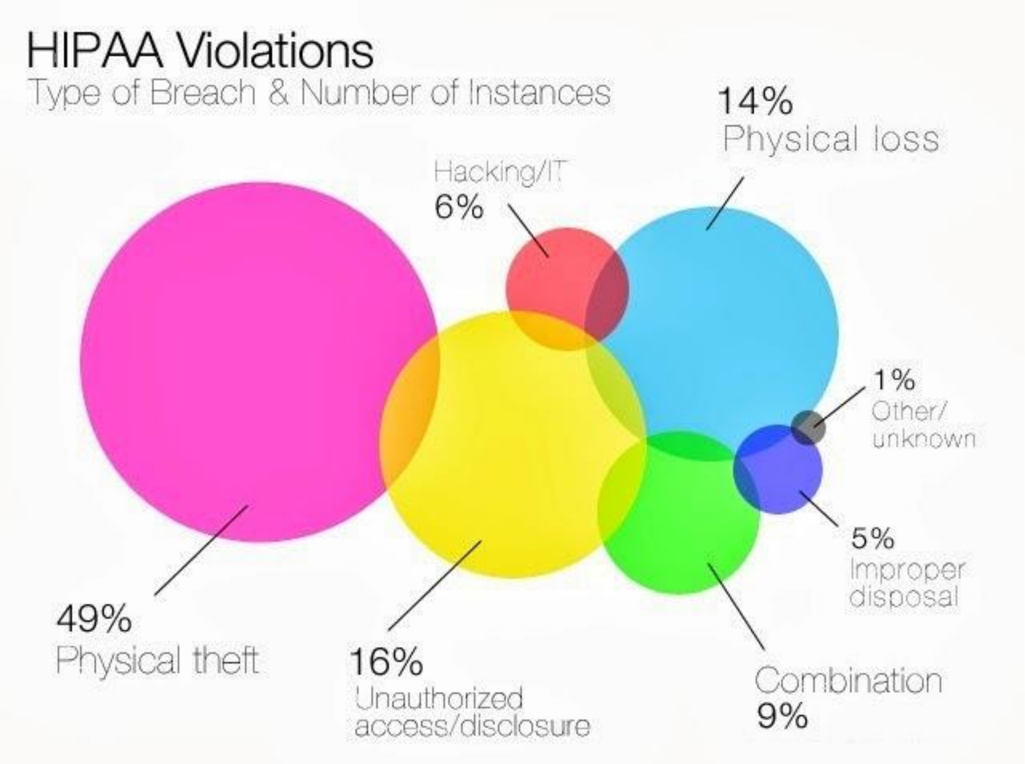
- Breach involving 500 or more individuals:
  - Submit a report to the HHS secretary immediately
  - Complete public posting on the Health and Human Services (HHS) website
  - Alert local media if those affected reside in the same area
    - Media outlets will make the decision whether to cover, after 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 at the end of the calendar year
- Vendor must notify federal trade commission of breaches caused by their products or services
- Business associates must notify covered entity

# Breach Notification: Example 2009 vs. 2013 Rules

## HACKERS ACCESS HEALTH PLAN'S RECORDS CONTAINING PHI AND ENCRYPT DATA TO PREVENT PLAN FROM ACCESSING IT

- Hacker's goal to disrupt plan operations so greatly, the plan will pay for encryption key
- Hackers not interested in causing financial, reputational or other harm to the individual whose PHI is encrypted
- Perhaps not a breach under 2009 rules if no substantial risk of harm
- Is a breach under 2013 rules

# Statistics on HIPAA Breaches



# Security Breach Violation Types

TYPE I -- INADVERTENT OR UNINTENTIONAL DISCLOSURE

- Inadvertent, unintentional or negligent act which violates policy and which may or may not result in PHI being disclosed
- Disciplinary action for a Type I disclosure will typically be a verbal warning, re-education, and review and signing of the Confidentiality Agreement. However, disciplinary action is determined with the collaboration of the Privacy Officer, Director of Human Resources and the department manager

TYPE II – INTENTIONAL DISCLOSURE

- Intentional act which violates the organization’s policies pertaining to that PHI which may or may not result in actual harm to the patient or personal gain to the employee
- Breach notification processes will be followed as described in the Breach Notification Policy

# Penalties

## INCREASED PENALTIES FOR NON-COMPLIANCE (INCLUDING FOR BUSINESS ASSOCIATES)

| Conduct of covered entity or business associate | Penalty |
|---|---|
| Did not know and, by exercising reasonable diligence, would not have known of the violation | $112 to $55,910 per violation;<br>Up to $1,667,299 per identical violation per year |
| Violation due to reasonable cause and not willful neglect | $1,118 to $55,910 per violation;<br>Up to $1,667,299 per identical violation per year |
| Violation due to willful neglect but the violation is corrected within 30 days after the covered entity knew or should have known of the violation | Mandatory fine of $11,182 to $55,910 per violation;<br>Up to $1,667,299 per identical violation per year |
| Violation due to willful neglect and the violation was not corrected within 30 days after the covered entity knew or should have known of the violation | Mandatory fine of not less than $55,910 per violation;<br>Up to $1,667,299 per identical violation per year |

# Criminal Penalties

***UNITED STATES V. RITA LUTHRA, M.D*. (D. Ma., May 1, 2018)**

- Background:
  - Doctor frustrated that some insurance companies won't cover her patients' prescriptions for certain osteoporosis drugs (Actonel and Altevia).
  - Doctor enlists the drug company's sales rep to develop prior authorizations.  Doctor directed medical assistant to share patient files (PHI) with the sales rep for the prior authorizations.
  - However, doctor did not get authorization from patients before sharing PHI with the sales rep.
- Court Proceedings:
  - Federal prosecutors charge doctor with HIPAA violation*.
  - Federal judge refuses to dismiss the HIPAA charges.
  - Jury ultimately convicts the doctor on the HIPAA charges.
- **<u>Doctor could be sentenced to one year in prison and a $50,000 fine for violating HIPAA.</u>**

** Federal prosecutors also charged the doctor with receiving $23,500 in illegal kickbacks from the drug company and for obstruction of justice / witness tampering (telling the medical assistant to lie to federal investigators).*

# EXAMPLES

# Example 1

I am an HR Business Partner.  I receive a call from Charlie Brown stating that he is reviewing the utilization reporting and wants all of the specific information regarding the high amount claimants. I am not familiar with Charlie (because I live under a rock), how should I handle this request?

# Solution 1

1. Tell Charlie Brown you need to investigate the situation and will call him back
2. Contact your Department head and verify that Charlie is entitled to the information
3. If approved to share information, limit your disclosure to the minimum necessary
4. Follow any policies and procedures for use, disclosure, documenting and storing any of PHI used

# Example 2

I am a call center employee and  receive a call from an employee, Miss Piggy. She needs assistance in resolving a claim for her husband, Kermit. She does not have any specific details regarding the services done, only a date of service and that the claim was denied.

# Solution 2

1. Take the information from Miss Piggy and obtain an authorization form that allows you to share the information with the provider or HR manager.  The service was for counseling

2. Recommend the employee use Health Advocate or their benefits provider to resolve the issue

3. Miss Piggy did not exhibit a familiarity with Kermit’s (her husband’s) treatment, you should not release any details about why it was declined to Miss Piggy

4. Contact the HR manager to discuss.  The safest route is to discuss the situation with her husband or secure an authorization to talk to Miss Piggy

# Example 3

I am an employee relations specialist and I receive an e-mail from an employee. The e-mail is a description of a specific claims issue. Apparently, an employee is fighting a substance abuse problem and is having difficulty getting claims paid. The e-mail contains information, including the employee’s name and social security number, it also has many specific details regarding the medical history of the individual. I am a little freaked out by the amount of detail in the e-mail.

# Solution 3

1. We can’t control how EPHI is sent to us

2. We should instruct employees that PHI should not be sent with details via e-mail as it offers very little protection en route to us

3. Once I receive the data, I must protect it.  I can encrypt the e-mail as I forward it on to the carrier or broker (where appropriate)

4. I can also notify the employee of the claim resolution using an encrypted e-mail.  I should save a copy of the e-mail only in a secure electronic, limited-access file

# Quiz Time

A. Employee contacts the HR Solutions Center at the direction of their manager because they have been sick all week. In their email they provide details of their symptoms, medicines they are taking and mention that their health care provider has advised that they should stay out of the office for at least a week.

B. Employee sends copy of completed Certification of Health Care Provider to HRSC instead of sending it to the LOA Coordinator directly.

C. Employee sends email to manager, who forwards to HRSC. Email contains information about a flare-up an employee is having as a result of cancer treatments, including diagnosis information.

D. Employee calls into HRSC for help registering for benefits, they disclose information about their chronic illness and want help selecting a medical plan that will cover necessary prescriptions and medical care.

## Answers

- Only “D” presents no HIPAA or state privacy law issues. Why?

- What issues arise in examples A-C?

- What should happen if an email containing PHI or other sensitive information is sent to a manager? To HRSC?

# Practical Tips

- Minimum necessary
- “Hands-off” approach to PHI
- PHI disclosures permitted for:
  - Enrollment information
  - Summary health information
  - De-identified information
  - Written authorization
- You are responsible for maintaining the privacy of our employees’ PHI and e-PHI
- Think before you disclose PHI or e-PHI – is it permitted?
- When you disclose PHI or e-PHI, make sure the person is the appropriate person or have an authorization form
- Use care in maintaining and using PHI and e-PHI
- If there is ever a doubt in your mind, ask before disclosing specific information

# QUESTIONS?

- For additional information see:
- http://www.cms.hhs.gov/SecurityStandard/
- http://www.hhs.gov/ocr/privacy/HIPAA/understanding/index.html

**Christopher K. Bao, Esq.**
Director of Employee Health and Benefits Compliance & Regulatory Affairs
Marsh & McLennan Insurance Agency Company, LLC
chris.bao@marshmma.com
(415) 230-7224