HIPAA, PRIVACY AND SECURITY FUNDAMENTALS

Greater Chattanooga ARMA

Presented by: Sue Gray, RHIA

SH Data Technologies

April 11, 2019

SH DATA TECHNOLOGIES

OBJECTIVES

- **Basic requirements of HIPAA**
- **What information is protected**
- **Practical privacy and security policies and guidelines for compliance**
- **Responsibilities of Business Associates**
- **How the rules are enforced**
- **HITECH Act and Final HIPAA Rule**

SH DATA TECHNOLOGIES

GLOSSARY OF TERMS

HIPAA – Health Insurance Portability and Accountability Act of 1996

OCR – Office of Civil Rights

HHS – Department of Health and Human Services

HITECH Act– Health Information Technology for Economic and Clinical Health Act

EDI – Electronic Data Interchange

SH DATA TECHNOLOGIES

WHAT IS HIPAA?

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

- **HIPAA includes:**
  - **Portability Rules ➡**
  - **Administrative Simplification ➡**

- **Goal = protect personal information**

SH DATA TECHNOLOGIES

PRIVACY RULE PROVISIONS

- **Standards for access, use and disclosure of PHI**
- **Individual rights regarding access, use and disclosure of PHI and right to receive notice of privacy practices**
- **Administrative requirements**
- **Health plan sponsor compliance obligation varies depending on**
  - Self-insured vs. fully-insured
  - Access to PHI for plan administration

SH DATA TECHNOLOGIES

WHAT IS PERSONALLY INDEFINABLE HEALTH INFORMATION (PHI)?

- **Any Healthcare Information that identifies the individual**

Or

- **Reasonable basis to believe can identify the individual**

SH DATA TECHNOLOGIES

WHAT IS COVERED?

- All Formats
- All Health Records - past, present, or future
  - Physical, mental health, or condition of an individual
  - All Health care provided to an individual
- Payment for health care

SH DATA TECHNOLOGIES

INDIVIDUAL RIGHTS

- **Inspect and copy their own PHI**
  - individual's right to access electronic PHI
- **Amend or correct incorrect or incomplete PHI**
- **Obtain an accounting of disclosures**
- **Receive a notice of privacy practices**
- **Request restrictions on use or disclosure of PHI**

SH DATA TECHNOLOGIES

WHO MUST COMPLY?

- **HIPAA applies to Covered Entities**
- **Contractual obligations imposed on Business Associates**
  - HIPAA regulates what contracts must include
- **HITECH Act ➔ many parts of the law now apply directly to Business Associates**

SH DATA TECHNOLOGIES

WHAT IS A COVERED ENTITY?

- Health related organizations that include, but are not limited to:
  - Any health plan
    - Insured and self insured plans
    - Healthcare Vendors and HMOs
    - Private sector plans
    - Government plans (Medicare and Medicaid)
- Healthcare Clearing House – may include medical billing service providers
- Healthcare Providers

SH DATA TECHNOLOGIES

HOW CAN AN EMPLOYER BE A COVERED ENTITY?

- Handling PHI that is protected under HIPAA
  - Health Clinic Operations
  - Company Nurse
  - Wellness Program
  - Self-Insured Health Plans
  - Acts as Intermediary between employees and healthcare providers

SH DATA TECHNOLOGIES

HOW MUST A COVERED ENTITY PROTECT PHI?

- Secure the PHI
- Written PHI privacy procedures
- Designate a Privacy Officer
- Require Business Associates to sign BAA
- Train Employees
- Provide written Privacy Practices

SH DATA TECHNOLOGIES

BUSINESS ASSOCIATES

- **Covered Entities work with certain service providers who may be Business Associates**

- **Covered Entities can disclose PHI to Business Associates if there is a Business Associate Agreement in place**

SH DATA TECHNOLOGIES

BUSINESS ASSOCIATE – DEFINITION

- **Person who (on behalf of a Covered Entity) creates, receives, maintains or transmits PHI**
- **A person who provides services to or for a Covered Entity, if the services involve use or disclosure of PHI**

SH DATA TECHNOLOGIES

BUSINESS ASSOCIATES REQUIREMENTS

- **Implement safeguards to protect confidentiality, integrity and availability of PHI/ePHI**
- **Ensure that any subcontractor implements appropriate safeguards**
- **Report security incidents to Covered Entity**

SH DATA TECHNOLOGIES

BUSINESS ASSOCIATE AGREEMENTS

- **Establish permitted uses and disclosures**
- **Prohibit improper use or disclosure**
- **Require appropriate safeguards**
- **Require reporting of unauthorized use or disclosure**

SH DATA TECHNOLOGIES

HIPAA SECURITY RULE

- **Standards for protecting maintained ePHI and Paper Documents**

- **Must implement safeguards to:**

  Ensure confidentiality, integrity and availability of ePHI and Paper Records

  Protect against reasonably anticipated threats to security and impermissible uses or disclosures

  Ensure compliance by workforce

SH DATA TECHNOLOGIES

SECURITY STANDARDS

- **Must comply with specific security standards**
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
- **Must perform a risk analysis**
  - Implementation specifications
  - Required vs. addressable
  - Flexibility
- **HITECH Act –security standards now directly apply to Business Associates**

SH DATA TECHNOLOGIES

WHAT ARE THE BEST METHODS TO PROTECT PHI?

- **Encrypted At Rest, In Transit, & Back-up**
  - At Rest not currently required but considered a Best Practice
- **Portable Device Usage**
  - Password Protected
  - When Offsite – must be maintained in a secure and HIPAA compliant manner
- **Lost/Stolen Electronic Devices**
  - Remote wiping
  - Hard Drive Encryption

SH DATA TECHNOLOGIES

WHAT ARE THE BEST METHODS TO PROTECT PHI?

- **Protect against reasonably anticipated threats to security and impermissible uses or disclosures**
  - **Encrypt**
    - Fax/E-mail
    - Portable Devices
    - Flash Media
    - Portable Media
- **Record and examine system activity for auditing purposes**

SH DATA TECHNOLOGIES

WHAT ARE THE BEST METHODS TO PROTECT PHI?

WORKFORCE COMPLIANCE:

- **Individual User Names and Passwords**
- **Access limited to minimum required to perform job**
- **Annual HIPAA Training**
- **Incorporate HIPAA Regulations into Policies and Procedures**

SH DATA TECHNOLOGIES

WHAT ARE THE BEST METHODS TO PROTECT PHI?

- Use Privacy Screen
- Use only secure Wi-Fi connections
- Use a secure Virtual Private Network (VPN)
- Reduce risks posed by third-party apps
- Securely delete all PHI stored on device before discarding or reusing
- Include Training on how to securely use mobile devices in workforce training programs

SH DATA TECHNOLOGIES

DESTRUCTION OF PHI

- **Paper PHI (any paper-based document)**

- **Electronic PHI (disks, e-mails, files)**

SH DATA TECHNOLOGIES

HIPAA, PRIVACY AND SECURITY FUNDAMENTALS 2.0

Greater Chattanooga ARMA

Presented by: Sue Gray, RHIA

SH Data Technologies

January 14, 2020

SH DATA TECHNOLOGIES

WHEN IS A PATIENT AUTHORIZATION REQUIRED?

- Not Required for disclosure for Treatment, Payment, or Health Care Operations

- Required when PHI is disclosed for any other Purpose

SH DATA TECHNOLOGIES

WHEN DISCLOSING PHI, CONSIDER

- ✓ **Minimum necessary standard**
- ✓ **Health Care Plan amendment required for plan sponsor to receive PHI**

SH DATA TECHNOLOGIES

ARE THERE EXCEPTIONS TO THE PRIVACY RULE?

It is possible to disclose PHI without an Authorization

SH DATA TECHNOLOGIES

ARE EMPLOYMENT RECORDS PROTECTED?

- **Privacy Rule does not protect employment records.**
- **If work for health plan or provider,**
  - **Does protect your medical and health plan records if**
    - **patient of the provider**
    - **member of health plan**

SH DATA TECHNOLOGIES

WHAT INFORMATION IS PROTECTED?

- **GENERALLY DOES NOT APPLY TO EMPLOYERS**
  - **IMPACTED WHEN OBTAINING HEALTHCARE RECORDS**
  - **EMPLOYEE BENEFITS**
  - **EMPLOYMENT RECORDS**

SH DATA TECHNOLOGIES

WHAT INFORMATION IS PROTECTED?

- **Workers Compensation**
  - **May disclose as allowed by State Law**
  - **Does Not require Authorization**

SH DATA TECHNOLOGIES

WHAT INFORMATION IS PROTECTED?

- **FMLA and ADA**
  - **No specific exception in HIPAA**
  - **Requires valid authorization**

SH DATA TECHNOLOGIES

HOW ARE COURT ORDERS HANDLED?

- **Court Orders**
  - **Permissible Disclosure**
  - **Includes Administrative Tribunal**
  - **Limited to information specifically described in the Order**

SH DATA TECHNOLOGIES

HOW ARE SUBPOENAS HANDLED?

- **May disclose only if the notification requirements of Privacy Rule are met**
- **Need proof of reasonable efforts to:**
  - **Notify person and allow:**
    - **Objection or**
    - **Seek Protective Order**

SH DATA TECHNOLOGIES

WHAT ABOUT MENTAL AND BEHAVIORAL HEALTH RECORDS?

- **Mental Health Records**
- **Substance Use Disorder Treatment Records**

SH DATA TECHNOLOGIES

WHAT ABOUT SCHOOL RECORDS?

- **Generally, No**
- **But, it could be, Yes**

SH DATA TECHNOLOGIES

ARE DOCTOR'S NOTE/HEALTH INFORMATION REQUESTS PROTECTED?

- **Requests from Employee - Not Covered**

- **Requests from Employer directly to Health Care Provider – Requires a valid authorization, unless another law allows**

SH DATA TECHNOLOGIES

ARE WELLNESS PROGRAM RECORDS PROTECTED?

Firewall between those working with wellness issues and those making employment decisions.

SH DATA TECHNOLOGIES

WHAT ABOUT EMPLOYEE CLINICS OR COMPANY NURSES?

Firewall between those working with health issues and those making employment decisions.

SH DATA TECHNOLOGIES

WHAT INFORMATION IS PROTECTED?

- **OSHA Logs**
  - **Required by Federal Law to disclose**
  - **Does Not require Authorization**

SH DATA TECHNOLOGIES

WHAT OTHER INFORMATION IS PROTECTED?

- **American Reinvestment and Recovery Act of 2009**
  - **HITECH Act**

  - **Disclosure may require patient authorization**

SH DATA TECHNOLOGIES

WHAT IS A BREACH?

Impermissible use or disclosure presumed to be breach unless can show through risk assessment there is a low probability PHI has not been compromised

- **Exceptions –**
  - No retention of information
  - Certain unintentional, internal disclosures
  - Certain inadvertent disclosures among people authorized to access PHI

SH DATA TECHNOLOGIES

WHAT RISK FACTORS ARE CONSIDERED TO DETERMINE IF A BREACH?

- Nature and extent of PHI involved;
- Unauthorized person who received or used PHI;
- Whether PHI was actually acquired or viewed; and
- Extent risk to PHI has been mitigated.

SH DATA TECHNOLOGIES

UNSECURED PHI

- **Breach notification rule applies only to breaches of unsecured PHI**
  - **PHI not secured by a technology or methodology approved by HHS**
  - **Must render PHI unusable, unreadable or indecipherable to unauthorized individuals**

SH DATA TECHNOLOGIES

SECURITY BREACH NOTIFICATION

- **Created by HITECH Act**
- **Requires notification of individuals whose unsecured PHI has been breached**
- **If breach involves PHI held by a Business Associate, the Business Associate must notify the Covered Entity**
- **Must notify HHS of breaches and, in some cases, the media**

SH DATA TECHNOLOGIES

PROVIDING NOTICE OF BREACH

- **Deadline for notice: without unreasonable delay and no later than 60 days**
- **Must be in writing and delivered via first class mail**
- **Provide notice to media outlets if breach affects more than 500 individuals in a particular area**

SH DATA TECHNOLOGIES

CONTENT OF NOTICE

- **Description of the breach**
- **Type of PHI involved**
- **Steps individuals should take to protect themselves from potential harm resulting from the breach**
- **Steps the Covered Entity/Business Associate is taking to investigate breach, mitigate losses and protect against future breaches**
- **Contact information for individuals to ask questions**

SH DATA TECHNOLOGIES

WHAT HAPPENS IF YOU BREAK HIPAA RULES?

Four potential outcomes

- **Handled internally**
- **Termination of Employment**
- **Professional Board Sanctions**
- **Criminal Charges including fines and imprisonment**

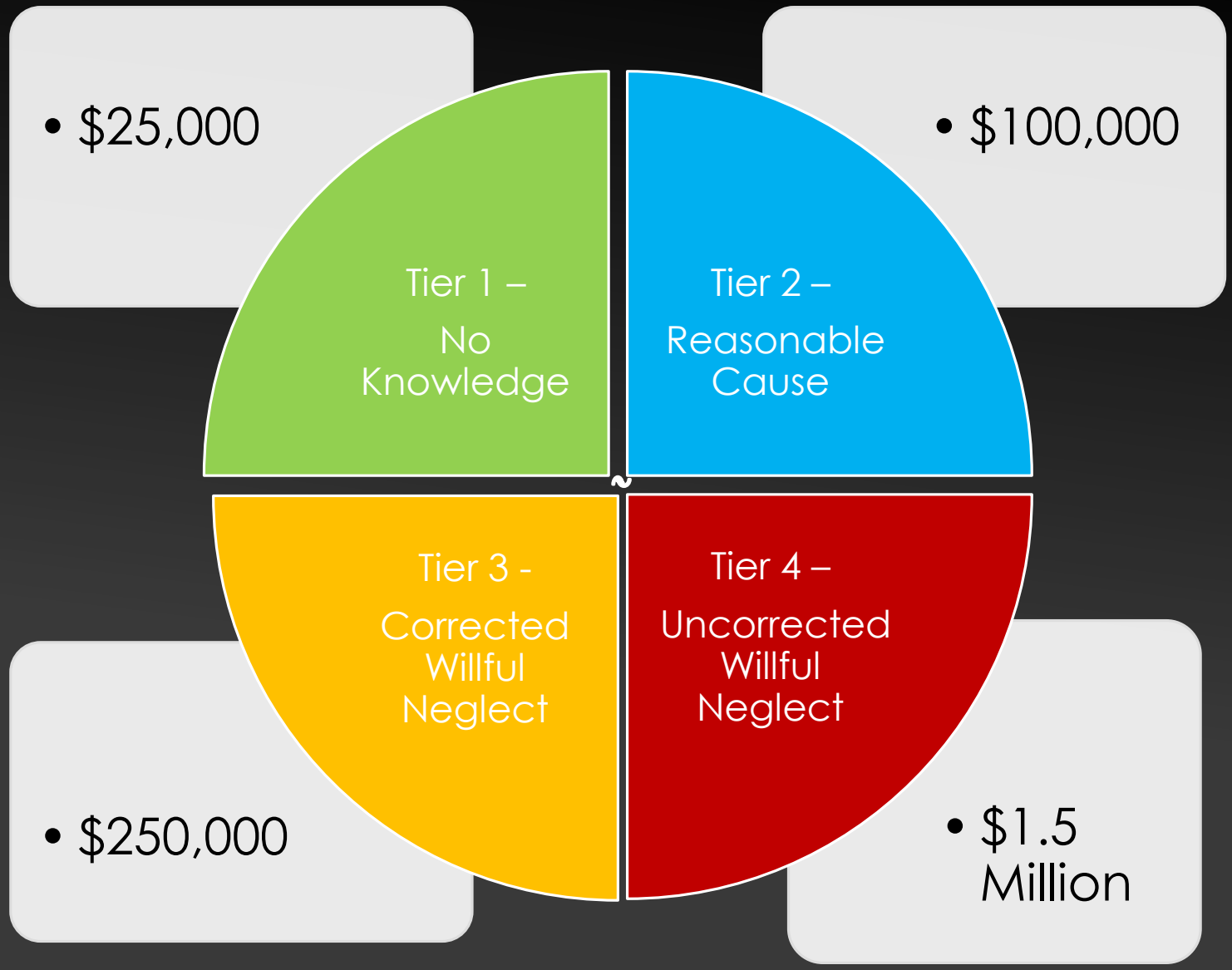
SH DATA TECHNOLOGIES

WHAT HAPPENS IF YOU BREAK HIPAA RULES?

Depends of the Severity of the Violation

- Nature of Violation
- Knowledge that violation occurred
- Whether Action was taken to Correct
- Malicious Intent/Personal Gain
- Harm caused
- Number of People impacted
- Violation was criminal provision of HIPAA

SH DATA TECHNOLOGIES



MONETARY CAPS FOR VIOLATIONS

SH DATA TECHNOLOGIES

WHAT CRIMINAL PENALTIES APPLY TO VIOLATIONS?

- **$50,000 fine and up to one year in prison for a willful violation**
- **Up to $100,000 fine and up to five years in prison for a violation committed under false pretenses**
- **Up to $250,000 fine and up to 10 years in prison for a violation with the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm**
- **Also, Mandatory two-year jail term for aggravated identity theft**
- **Now applies to anyone who improperly uses/discloses PHI, not just Covered Entities and their employees**

SH DATA TECHNOLOGIES

IS HIPAA PRIVACY RULE SUSPENDED DURING A NATIONAL OR PUBLIC HEALTH EMERGENCY?

No

Certain Provisions can be waived

SH DATA TECHNOLOGIES

WHAT ABOUT STATE LAWS?

Tennessee State Law:

TCA 47-18-2107 – Does not apply if subject to HIPAA

SH DATA TECHNOLOGIES

WHAT ARE THE MOST COMMON HIPAA VIOLATIONS?

- Employees disclosing information
- Medical records mishandling
- Lost or Stolen Devices
- Texting patient information
- Social Media
- Employees illegally accessing files
- Social Breaches
- Authorization Requirements
- Accessing PHI on home computers
- Lack of Training

SH DATA TECHNOLOGIES

WHAT ARE OTHER HIPAA VIOLATIONS?

- Malware Incident
- Ransomware Attack
- Hacking
- Business Associate Breach
- EHR Breach
- Office Break-in

SH DATA TECHNOLOGIES

COMMON CATEGORIES FOR HIPAA VIOLATIONS

- Uses and disclosures
- Improper security safeguards
- The Minimum Necessary Rule
- Access controls
- Notice of Privacy Practices

SH DATA TECHNOLOGIES

WHAT IS THR BEST DEFENSE AGAINST VIOLATIONS?

- Privacy and Confidentiality always a priority
- Annual Staff Training
- Incorporate HIPAA regulations into policies and procedures
- Effective Compliance Program

SH DATA TECHNOLOGIES

WHAT DO I NEED TO DO?

Three objectives:

1) **Keep records confidential**
2) **Maintain integrity of the records**
3) **Ensure authorized individuals may access records as needed**

SH DATA TECHNOLOGIES

QUESTIONS

Thank you for your time and attention

SH DATA TECHNOLOGIES

RESOURCES

American Health Information Management Association - ahima.org

Department of Health and Human Services – HHS.gov

Office of Civil Rights – hhs.gov/civil- rights

SH DATA TECHNOLOGIES

CONTACT INFORMATION

Sue Gray, RHIA

Corporate Compliance

SH Data Technologies

865-314-7458

sgray@shdatatech.com

SH DATA TECHNOLOGIES