ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

PREPARING FOR THE INEVITABLE

Best Practices for Preventing, Investigating, and Responding to HIPAA Security Incidents and Breaches

Denise M. Leard, Esq.
Brown & Fortunato

TOPICS

- What Do You Think?
- Key Definitions
- General Rules Under HIPAA
- State Privacy Laws
- Breaches
  - Identify a Breach
  - Reporting a Breach
- Tips & Lessons Learned

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

KEY DEFINITIONS

HIPAA, Protected Health Information (PHI), Covered Entities, and Business Associate

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

- Enacted in 1996 to address privacy and security concerns with use and disclosure of "protected health information" by "covered entities"
- Implementing regulations include the "Privacy Rule," "Security Rule," and the "Breach Notification Rule," located in Title 45 of the Code of Federal Regulations

HIPAA – COVERED ENTITIES

- Health Plans
- Health care providers transmitting health information in electronic form in connection with a covered transaction, and
- Health care clearinghouses
(i.e., companies that process/transmit health information)

HIPAA – PROTECTED HEALTH INFORMATION

- PHI is information, including demographic data, that relates to:
  - The individual's past, present, or future physical or mental health or condition,
  - The provision of health care to the individual, or
  - The past, present, or future payment for the provision of health care to the individual
- And identifies or could reasonably be used to identify the individual

IS IT PHI?

- Intake paperwork that includes patient's first and last name, treating physician, and primary diagnosis. Paperwork does not include patient's date of birth, insurance information, or social security number.
- Email from intake personnel that says: "We received Robert Jackson's medical records from the hospital."
- Text from intake personnel that says: "We received RJ's medical records from the hospital."
- Email sent from provider to djones@hotmail.com. Email states: "Our agency will have a booth at the health fair on Saturday. We hope you can stop by to see us!"
- Email sent from provider to djones@hotmail.com. Email states: "Dear Ms. Jones: We received a new order for you from Dr. Smith."

HIPAA – BUSINESS ASSOCIATE

- A Business Associate is
  - A person or organization that performs certain functions or activities on behalf of a Covered Entity that involve the use or disclosure of PHI
    - Business Associate functions include claims processing, data analysis, utilization review, and billing
    - Business Associate services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services
- A Business Associate does not include
  - A person or organization who performs functions or services that do not involve the use or disclosure of PHI and where any access to PHI by such person would be incidental, if at all

IS IT A BUSINESS ASSOCIATE?

- USPS, UPS, FedEx, and other delivery services employees?
- Software vendors?
- Janitors?
- Plumbers, electricians, or photocopy machine repairmen who provide repair services in a covered entity's office?
- Shredding service?
- Attorney?

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

GENERAL RULES UNDER HIPAA

Privacy Rule, Security Rule, and Breach Notification Rule

HIPAA

- Privacy Rule
  - Permitted uses and disclosures of PHI
  - Notice of Privacy Practices
  - Right to access, amend, restrict, and receive accounting of disclosures
- Security Rule
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
  - Policies and documentation

HIPAA

- Breach Notification Rule
  - Breach
  - Reporting requirements

HIPAA PRIVACY RULE

- Authorization
  - In general, the HIPAA Privacy Rule requires an individual's authorization to use and disclose PHI unless the use or disclosure is expressly permitted in the HIPAA Privacy Rule
- Treatment, Payment, and Health Care Operations
  - Covered entities (and business associates on behalf of CEs) may use and disclose PHI for treatment, payment and health care operations of the covered entities

WHAT USES AND DISCLOSURES OF PHI ARE ALLOWED WITHOUT AN AUTHORIZATION?

- Required Disclosures
  - The disclosure is to the individual (or their personal representative) requesting his/her PHI or an accounting of disclosures
  - The Secretary of HHS requests access to information in order to determine compliance with HIPAA
- Permitted Disclosures
  - To the individual
  - TPO
  - Certain defined circumstances to benefit public interest

WHAT USES AND DISCLOSURES REQUIRE AUTHORIZATION?

- If the disclosure is not for treatment, payment, health care operations, or as otherwise permitted by the HIPAA Privacy Rule, you must obtain a valid authorization to disclose the PHI
- Authorizations require:
  - Description of the information to be disclosed,
  - The name of the individual/entity authorized to make the disclosure,
  - The name of the individual/entity to whom the disclosure will be made,
  - Description of the purpose of the requested disclosure,
  - Expiration date or event, and
  - Signature of the individual and date.

IS AN AUTHORIZATION REQUIRED?

- A provider's website designer suggests that the provider include patient testimonials on the website. The testimonials will include a quote from the patient and a picture of the patient.
- A provider believes it is being underpaid by BCBS. The provider contacts BCBS's contract manager on behalf of our client. The contract manager requests a list of the claims in dispute. The contract manager wants the list to include each patient's name, date of service, diagnosis, and service provided.
- A home health agency sends a request for a patient's hospital records relating to a knee surgery that is the basis for the patient's home health services.

HIPAA SECURITY RULE

- Covered entities and their business associates must:
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures;
  - Implement administrative, physical and technical safeguards designed to protected e-PHI; and
  - Ensure compliance by their workforce.

HIPAA SECURITY RULE

- Three categories of standards: Administrative, Technical, and Physical Safeguards
- 18 Standards
- 12 Standards have Implementation Specifications
  - "Required"
  - "Addressable"
- Policies and Procedures

HIPAA SECURITY RULE - SAFEGUARDS

- Administrative Safeguards
  - HIPAA Privacy and Security Officer(s)
  - Training
  - Workforce Compliance and Sanctions
  - Procedures for Security Incidents
  - Contingency Plans and Emergency Procedures
  - Reviewing Information Security Systems
  - Risk Analysis

HIPAA SECURITY RULE - SAFEGUARDS

- Physical Safeguards
  - Policies and procedures regarding access to facilities and devices
  - Managing and securing devices containing PHI
- Technical Safeguards
  - Automatic logoff procedures
  - Emergency access procedures
  - Encryption/decryption techniques
  - Audits of hardware and software
  - Person/entity identity verification

HIPAA BREACH NOTIFICATION RULE

- Breach
  - "… acquisition, access, use or disclosure of protected health information in a manner not permitted under" the Privacy Rule "which compromises the security or privacy of protected health information"
- Notification
  - Individual
  - Office for Civil Rights (OCR)
  - Media

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

STATE PRIVACY LAWS

STATE PRIVACY LAWS

- HIPAA is a minimum set of standards that must be followed.
- In the event of a conflict with state law, the more stringent law will apply.

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

BREACHES UNDER HIPAA

What is the likelihood? What are common causes?
Is a breach the same as a violation of HIPAA?
How do you determine whether a breach occurred?
What notices are required?

WHAT'S THE LIKELIHOOD OF A BREACH?

- OCR 201 Desk Audits
  - 94% of organizations had inadequate risk management plans
  - 83% of organizations had performed inadequate risk analysis
  - 89% of organizations were inadequate on patient's right to access
- 90% of health care organizations experience at least one data breach within a 2-year period. Half of those organizations experience more than 5 data breaches within a 2-year period.

COMMON CAUSES OF BREACHES

- Third Parties
  - 41% of breaches experienced by covered entities
- Unintentional Employee Actions
  - 36% of breaches experienced by covered entities
  - 55% of breaches experienced by business associates

IS BREACH A 4-LETTER WORD?

- Not necessarily – A breach is NOT equivalent to a HIPAA violation that can result in significant fines and penalties
- Failing to report a breach and/or failing to take steps to prevent breaches will likely result in serious consequences for covered entities and business associates

CIVIL PENALTIES FOR HIPAA VIOLATIONS

- Tier 1
  - Did not know and could not have reasonably known of violation
  - $100 - $50,000 per violation; maximum of $25,000 per year
- Tier 2
  - Reasonable cause to believe knew/should have known of violation
  - $1,000 - $50,000 per violation; maximum of $100,000 per year

CIVIL PENALTIES FOR HIPAA VIOLATIONS

- Tier 3
  - Violation due to willful neglect but corrected within 30 days
  - $10,000 - $50,000 per violation; maximum of $250,000 per year
- Tier 4
  - Violation due to willful neglect and not corrected within 30 days
  - $50,000 per violation; maximum of $1.5 million per year

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

IDENTIFY A BREACH

IDENTIFY A BREACH

- What is a breach?
  - The unauthorized, "… acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information"
- Four Key Questions:
  - Was there an unauthorized acquisition of, access to, or use or disclosure of PHI?
  - Was the PHI unsecure?
  - Does an exception to the definition of breach apply?
  - Can the entity demonstrate a low probability that the PHI has been compromised?

IDENTIFY A BREACH

- Question 1 – Was there an unauthorized acquisition of, access to, or use or disclosure of PHI?
  - To answer this question, it is necessary to understand a few terms
    - Protected Health Information
    - Unauthorized
    - Acquisition/Access/Use/Disclosure

IDENTIFY A BREACH

- Question 2 – Was the PHI unsecure when it was acquired/accessed/used/disclosed?
- PHI is secure if it is either
  - Appropriately encrypted (i.e. converted into encoded or unreadable text that requires a confidential process or key to assign meaning), or
  - Properly destroyed.
- OCR has cautioned about the limits of full disk encryption
  - Laptop with full disk encryption – security of PHI depends on if the laptop was powered on and in use or was powered off.

IDENTIFY A BREACH

- Question 3 – Does an exception to the definition of breach apply?
  - There are three exceptions under the Breach Notification Rule
    - Unintentional acquisition, access, or use of PHI by a workforce member made in good faith, was within the scope of authority, and does not result in further inappropriate use or disclosure
    - Inadvertent disclosure of PHI by an authorized person to another person authorized to access PHI at the same covered entity or organized health care organization and does not result in further inappropriate use or disclosure
    - Disclosure of PHI where the entity has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information

IDENTIFY A BREACH

- Question 4 – Can the entity demonstrate a low probability that the PHI has been compromised?
  - Presumption
    - If there was an unauthorized acquisition, access, use, or disclosure of PHI and no exception applies, then the incident is presumed to be a breach unless the entity can demonstrate that there is a low probability that the PHI has been compromised

REPORTING A BREACH

- General Notice Requirement
  - Written notice sent by first-class mail or by email if the affected individual has agreed to electronic notice
  - Without unreasonable delay but in no case more than 60 days after discovery of the breach
- Substitute Notice
  - Are there 20 or more affected individuals with insufficient contact information?
    - If yes, either post notice on the homepage of the entity's Website for 90 days or provide notice in major print or broadcast media where the affected individuals likely reside
    - If no, provide substitute notice to those individuals by alternative written means, telephone, or other means

REPORTING A BREACH

- Content of Individual Notice
  - Description of incident
  - Description of PHI involved
  - Steps that can be taken to protect against potential harm
  - Description of investigation undertaken
  - Steps taken to mitigate harm and protect against future breaches
  - Contact information

REPORTING A BREACH

- Notice to OCR and others
  - Did the breach affect 500 or more individuals?
    - If yes, provide notice to OCR when notifying individuals and media outlets
    - If no, submit online breach notification to OCR or include in breach log submitted annually to OCR by March 1 of the following calendar year.
- Notice to media
- State law breach reporting
  - All states have laws governing patient privacy and require reporting of certain breaches
  - Such laws may be stricter than HIPAA and should be reviewed in the event of a breach to ensure compliance

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

TIPS AND LESSONS LEARNED

Tips for responding to breaches and lessons learned from recent settlements with OCR

RESPONDING TO A POTENTIAL BREACH

- Assemble a team
  - The team should include high level personnel and others as necessary
  - It may be necessary to involve an attorney to keep the investigation privileged
  - If the breach involves electronic data or systems, a computer forensic consultant may be necessary
  - If the breach is large, a public relations company may be useful to minimize negative press for the company

RESPONDING TO A POTENTIAL BREACH

- Investigate, analyze, and take action
  - Gather information and interview employees
  - Take steps to maintain confidentiality and preserve evidence
  - Mitigate harm
  - Develop and implement a corrective action plan (including an update to the entity's risk analysis and management plan)
  - Involve law enforcement?
  - Notify insurance carriers?
  - Determine what kind of breach reporting will be required
  - Document the company's investigations and actions

LESSONS LEARNED

- Jackson Health System (JHS)
  - October 15, 2019
  - OCR alleged JHS violated the HIPAA Security and Breach Notification Rules between 2013 and 2016
    - JHS failed to timely provide breach notification
    - JHS failed to conduct an enterprise-wide risk analysis and manage identified risks
    - Routinely review information system activity records
    - Restrict employees' authorization to the minimum necessary for assigned job
  - OCR imposed a civil monetary penalty of $2,154,000 against JHS

LESSONS LEARNED

- Elite Dental Associates
  - October 2, 2019
  - OCR alleged Elite impermissibly disclosed PHI on a review/social media platform
  - Elite agreed to pay $10,000
- Touchstone Medical Imaging
  - May 6, 2019
  - OCR alleged Touchstone failed to thoroughly investigate, timely give notice of a breach, and to secure a business associate agreement
  - Touchstone agreed to pay $3,000,000 and adopt a corrective action plan

LESSONS LEARNED

- Pagosa Springs Medical Center (PSMC)
  - November 5, 2018
  - OCR alleged PSMC impermissibly disclosed PHI to a former employee and to a business associate without a BAA
  - PSMC agreed to pay $111,400 and adopt a corrective action plan
- St. Luke's-Roosevelt Hospital Center, Inc. (St. Luke's)
  - May 23, 2017
  - OCR alleged carelessly handled PHI and sensitive information resulting in an impermissible disclosure
  - St. Luke's agreed to pay $387,000 and implement a corrective action plan

LESSONS LEARNED

- The University of Texas MD Anderson Cancer Center (MD Anderson)
  - March 24, 2017
  - OCR alleged MD Anderson failed to adequately remediate and manage its own high-risk assessment regarding encryption or document reasons encryption was not feasible and implement an equivalent alternative
  - A civil monetary penalty of $4,348,000 was assessed
  - MD Anderson has filed a complaint with HHS and appealed the penalty to the United States Court of Appeals for the 5th Circuit

LESSONS LEARNED

- Presence Health
  - January 9, 2017
  - OCR alleged that Presence Health failed to timely notify affected individuals and the media following a breach
  - $475,000 settlement

FINAL TIPS

- Risk Assessment
  - Conduct and update security risk assessments
- Risk Management
  - Prepare and implement risk management plans
- Encrypt
  - Invest in (and use) encryption technology
- Train
  - Train employees

FINAL TIPS

- Investigate BAAs
  - Investigate business associates and strengthen rights with business associates
- BAA Agreements
  - Know who your business associates are and ensure you have current agreements in place
- Policies
  - Have policies and safeguards in place to ensure PHI is only disclosed when required or permitted under the law

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

QUESTIONS?

Email us at auweb@achcu.com

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

Thank You

Denise M. Leard, Esq.
Brown & Fortunato, P.C.
905 S. Fillmore St., Ste. 400
Amarillo, TX 79101
dleard@bf-law.com | 806-345-6318