ACHC U
EDUCATIONAL RESOURCES

DMEPOS

HIPAA: Lessons Learned

Denise M. Leard, Esq.
Brown & Fortunato

Topics

- Overview of HIPAA
  - Key Definitions
  - General Rules
- OCR Investigation and Informal Settlement Hot Topics
- Recent Cases, Actions, and Settlements

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

HIPAA

Key Definitions & General Rules

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

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

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

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

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 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

Recent Cases, Actions, and Settlements

Current Enforcement Stats

- 278,953 complaints received
- 97% resolved
  - 29,205 cases –required changes in practices, corrective action
  - 101 cases – CMP totaling $131,060,482
  - 13,413 cases – no violations
  - 49,874 cases - technical assistance given, no investigation needed
  - 179,054 cases – complaint did not present a case eligible for enforcement
- 1,226 referrals to DOJ

Complaints Filed

- Impermissible uses & disclosures of PHI
- Lack of safeguards for PHI
- Lack of patient access to their PHI
- Lack of administrative safeguards of ePHI
- Violation of minimum necessary rules

OCR Takes Breaches Seriously

- Excellus Health Plan Inc. agreed to pay $5.1 million January 15, 2021
  - In 2015, Excellus filed a breach report stating that cyber attacker had gained unauthorized access to its information technology systems.
  - Breach began on December 23, 2013, and ended on May 11, 2015, and Affected over 9.3 million people

* No private right of action under HIPAA

Dr. Stephen Porter

- March 3, 2020
- Dr. Porter filed a breach report with OCR related to dispute with business associate
- OCR investigated and found:
  - Never conducted a risk analysis before the breach
  - Never conducted one after the breach
  - Despite significant technical assistance from OCR, did not implement sufficient security measures
- $100,000 settlement
- Corrective action plan

Lessons Learned From Dr. Porter

- In business dispute, call your lawyer – not OCR
- Security risk assessment = REQUIREMENT
- If OCR gives you technical assistance, implement it

Sentara Hospitals

- Nov. 27, 2019
- OCR alleged Sentara Hospitals violated the HIPAA Breach Notification and Privacy Rules
  - Sentara Hospitals failed to notify OCR of a breach of unsecured PHI
  - Sentara Hospitals failed to have a business associate agreement with its parent company that created, received, maintained, and transmitted PHI on behalf of Sentara Hospitals
- Sentara Hospitals agreed to pay $2.175 million to settle the potential violations

Lessons Learned From Sentara

- Definition of PHI
- Breach analysis
  - Start with presumption of breach
  - 4 factors

Jackson Health System (JHS)

- Oct. 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 from Jackson Health System

- Fundamental Failure
  - Commitment
  - Leadership
  - Execution
  - Resources?
- Complete breach reports
- Employee training

Elite Dental Associates

- Oct. 2, 2019
- OCR alleged Elite impermissibly disclosed PHI on a review/social media platform
- Elite agreed to pay $10,000

Lessons Learned From Elite Dental

- Cannot respond to online complaints!
- Work with patient
- Report false or defamatory review to Yelp
- Court order

Right of Access Initiative

- "For too long, healthcare providers have slow-walked their duty to provide patients their medical records out of a sleepy bureaucratic inertia. We hope our shift to the imposition of corrective actions and settlements under our Right of Access Initiative will finally wake up healthcare providers to their obligations under the law."

  – Roger Severino, OCR Director

Right of Access Initiative

- Bayfront Health St. Petersburg – Sept. 9, 2019
  - PHI provided to patient 9 months after initial request
  - $85,000 payment
  - Corrective action plan
- Korunda Medical, LLC – Dec. 12, 2019
  - PHI not timely provided
  - PHI not provided in requested electronic format
  - Excessive charges for records
  - $85,000 payment
  - Corrective action plan

Right of Access Initiative

- Dr. Robert Glaser
  - OCR received a complaint from a former patient that Dr. Glaser failed to provide access to medical records.
  - Dr. Glaser failed to respond to multiple request for information from OCR
  - Accessed a civil monetary penalty of $100,000 for violation of right to access

Lessons Learned: Right of Access Initiative

- Complaints from patients OR their lawyers
- Provide records ASAP
- Resolve complaint immediately when OCR involved
- Understand what you can charge
  - Patient third-party directive vs. authorization
  - EMR vs. Designated Record Set

Touchstone Medical Imaging

- May 6, 2019
- OCR alleged Touchstone failed to thoroughly investigate, give timely 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 From Touchstone

- Vet your IT professionals
  - Bad configuration
  - No BAA
- Perform Security Risk Assessment
  - Insecurity of server undiscovered
- Take action once breach discovered
  - Mitigation
  - Proper notification

Pagosa Springs Medical Center

- 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 $111,400.00 and adopt a corrective action plan

Lessons Learned From Pagosa Springs

- Coordinate HR and IT when employee terminates
- Implement process to review all SaaS, programs and contracts
  - BAA needed?

Anthem, Inc.

- October 15, 2018
- Largest U.S. health data breach
- $16 million settlement
- 79 million individuals affected
- Spear phishing

Lessons Learned from Anthem

- Technical Safeguards: strong security program
  - Spam email detection program
  - Monitoring activities on your system
- Administrative Safeguards:
  - Training
  - Have mechanism for employees to report/determine authenticity of suspicious email
  - Test employees by sending phishing emails and see if they click
    - Retrain if they do

St. Luke's-Roosevelt Hospital Center, Inc.

- 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 From St. Luke's

- Never fax to an employer
- Clear policies
- Training, training, training!

University of Texas MD Anderson Cancer Center

- 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 From UT MD Anderson

- Follow through
- Where's your ePHI?
- Encryption=standard of care
  - Phones
  - Laptop/tablets
  - Thumb drives

Resources

- OCR Secures $2.175 Million HIPAA Settlement from Sentara Hospitals:: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/sentara/index.html
- OCR Imposes $2.15 Million Penalty Against Jackson Health System: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/jackson/index.html
- Elite Dental Associates Agreed to Pay $10,000 Settlement for PHI Disclosure: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/elite/index.html
- Bayfront Health St. Petersburg Agreed to Pay $85,000 Settlement for HIPAA Right of Access: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/bayfront/index.html

Resources

- Korunda Medical LLC Agreed to Pay $85,000 to OCR for Settlement for HIPAA Right of Access: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/korunda/index.html
- Touchstone Medical Imaging Agreed to Pay $3 Million to OCR for PHI Breach: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/tmi/index.html
- Pagosa Springs Medical Center Agreed to Pay $111,400 to OCR for Impermissible Disclosure of PHI: https://www.hhs.gov/about/news/2018/12/11/colorado-hospital-failed-to-terminate-former-employees-access-to-electronic-protected-health-information.html
- Anthem, Inc. Agreed to Pay $16 Million to OCR in Record HIPAA Settlement: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html

Resources

- St. Luke's-Roosevelt Hospital Center, Inc. Agreed to Pay $387,000 to HHS for Alleged Violations of Careless Handling of PHI: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/stlukes/index.html
- The University of Texas MD Anderson Cancer Center Assessed $4,348 Million Civil Monetary Penalty by Administrative Law Judge for HIPAA Violations (on appeal to the Fifth Circuit Court of Appeals):. The Univ. of TX MD Anderson Cancer Center, DAB CR5111 (2018); https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/mdanderson/index.html

Questions?

ACHC U®
EDUCATIONAL RESOURCES

Thank you

Denise M. Leard, Esq.
dleard@bf-law.com | 806-345-6318

Brown & Fortunato
Amarillo · Dallas