ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

HIPAA: Lessons Learned

Recent Cases, Enforcement Actions, and Settlements

Brown & Fortunato
Celebrating 25 Years Together

Presenters

Beth Anne Jackson, J.D.
Brown & Fortunato, P.C.
905 S. Fillmore, Ste. 400
Amarillo, TX 79101
bjackson@bf-law.com
806-345-6346

Allison D. Shelton, J.D.
Brown & Fortunato, P.C.
905 S. Fillmore, Ste. 400
Amarillo, TX 79101
ashelton@bf-law.com
806-345-6338

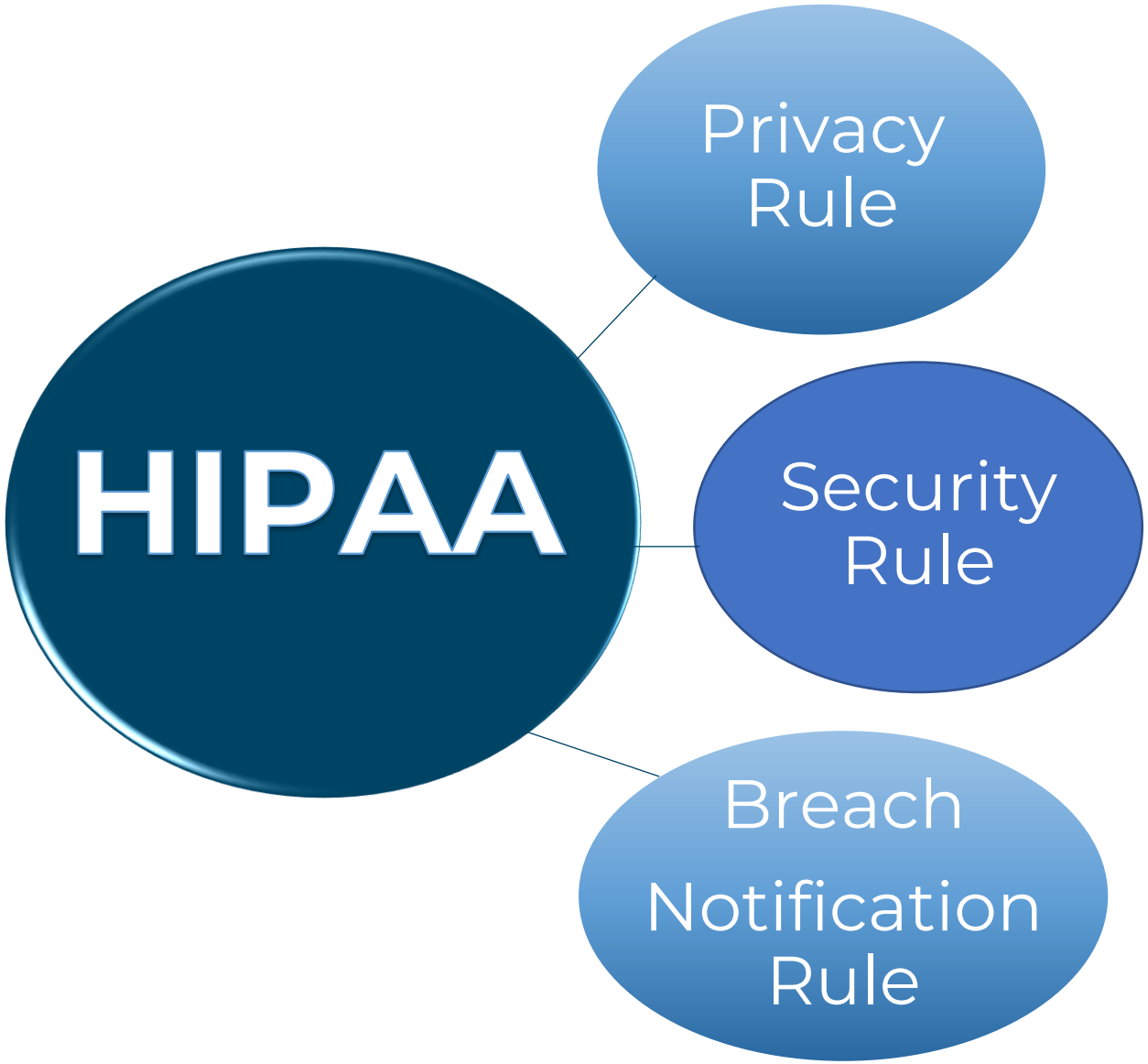
Board Certified, Health Law | Texas Board of Legal Specialization

Topics

- Overview of HIPAA:
- OCR Enforcement Statistics
- Recent Cases, Actions, and Settlements

HIPAA

Overview of General Rules



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

ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

Enforcement Statistics

Current Enforcement Stats

- 270,242 complaints received
- 99% resolved:
  - 29,031 cases – required changes in practices, corrective action.
  - 101 cases – CMP totaling $135,328,482.
  - 12,426 cases – no violations.
  - 49,156 cases - technical assistance given, no investigation needed.
  - 174,943 cases – complaint did not present a case eligible for enforcement.
- 1,167 referrals to DOJ.

Complaints Filed

- Common issues reported in complaints:
  - 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.
- Most common types of entities identified in complaints:
  - Hospitals
  - Private practices and physicians
  - Outpatient facilities
  - Pharmacies
  - Community Health Centers

Recent Enforcement Actions & Settlements

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

HIPAA Right to Access Initiative

No	Date	Resolution	OCR Allegations
20	9/10/2021	$80,000 CAP / 1 yr monitoring	Provider failed to timely provide complete set of minor's records after multiple requests from parent.
19	6/2/2021	$5,000 CAP / 2 yr monitoring	Provider failed to provide minor's records until 2 years after parent's request.
18	3/26/2021	$30,000 CAP/ 2 yr monitoring	Plastic surgery provider failed to timely provide records.
17	3/24/2021	$65,000 CAP/ 1 yr monitoring	After first complaint, OCR provided technical assistance to hospital. Later in the month, OCR received a second complaint regarding same records.
16	2/12/2021	$70,000 CAP / 2 yr monitoring	After first complaint, OCR provided technical assistance to health system. Two months later, OCR received a second complaint regarding same records.
15	2/10/2021	$75,000 CAP / 2 yr monitoring	Health system failed to timely respond to patient request that electronic copy of records be sent to third party.
14	1/12/2021	$200,000 CAP / 2 yr monitoring	Health system received to requests and did not provide records for 6 months in one case and 8 months in the other case.

HIPAA Right to Access Initiative

No	Date	Resolution	OCR Allegations
13	12/22/2020	$36,000 CAP/ 2 yr monitoring	After first complaint, OCR provided technical assistance to physician practice. Five months later, OCR received a second complaint regarding same records.
12	11/19/2020	$65,000 CAP/ 2 yr monitoring	AMC failed to timely provide electronic copy of records to patient's lawyer.
11	11/12/2020	$15,000 CAP / 2 yr monitoring	After first complaint, OCR provided technical assistance to physician. A year later, OCR received a second complaint regarding same records.
10	11/6/2020	$25,000 CAP / 2 yr monitoring	After first complaint, OCR provided technical assistance to physician practice. A month later, OCR received a second complaint regarding same records.
9	10/9/2020	$100,000 CAP / 2 yr monitoring	Medical practice withheld diagnostic images from records requested by patient.
8	10/7/2020	$160,000 CAP / 2 yr monitoring	Hospital did not provide all of minor's records requested by his mother.

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.

The New Frontier: Class Action Lawsuits

- March 4, 2021- Unity Health System Settlement:
  - Two data breaches, 1.4 million records of patients and employees, in 2017 and 2018.
  - Settlement includes credit monitoring and reimbursement of class members' expenses, lost time, and costs.
  - Attorneys' fees and expenses of up to $1.57 million.
  - No private right of action under HIPAA .

Lessons Learned Unity Health

- Comply with Timeframes for Notifications
  - Notice to the individual "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." 45 C.F.R. § 164.404.
  - Notice to OCR and the media
- Comply with Content Requirements for Breach Notification Letters
  - Description of breach (including date of breach and date of discovery)
  - Description of investigation
  - Types of PHI involved in the breach (e.g., name, SSN, DOB, address, diagnosis, etc.)
  - Steps the individual should take to protect against potential harm
  - Steps provider is taking to mitigate harm and to protect against future breaches
  - Contact information for additional information

Excellus Health Plan

- January 15, 2021:
  - Over the course of 17 months, cyber-attackers accessed the health plan's information system and installed malware resulting in the disclosure of PHI of 9.3 million individuals.
  - OCR investigated and found that the health plan:
    - Failed to conduct an enterprise-wise risk analysis.
    - Failed to implement risk management.
    - Failed to review information system activity.
    - Failed to implement access controls.
- Settlement:
  - $5.1 million and corrective action plan with 2 years of monitoring.

Lessons Learned from Excellus Health Plan

- *"Hacking continues to be the greatest threat to the privacy and security of individuals' health information. In this case, a health plan did not stop hackers from roaming inside its health record system undetected for over a year which endangered the privacy of millions of its beneficiaries. We know that the most dangerous hackers are sophisticated, patient, and persistent. Healthcare entities need to step up their game to protect the privacy of people's health information from this growing threat."*

  -OCR Director Roger Severino

- Security Risk Assessment, 45 C.F.R. § 164.308(a)(1)(ii)(A).
- Risk Management, 45 C.F.R. § 164.308(a)(1)(ii)(B).
- System Activity Review, 45 C.F.R. § 164.308(a)(1)(ii)(D).

CHSPSC, LLC

- September 23, 2020:
  - FBI traced cyber-hacking activity to CHSPSC's information system.
  - The unauthorized access did not cease until 4 months after FBI notified CHSPC.
  - The PHI of 6,121,158 individuals was accessed.
  - OCR investigated and found that CHSPSC:
    - Failed to comply with Security Rule over a long period of time.
    - Failed to review information system activity.
    - Failed to implement security incident procedures.
    - Failed to implement access controls.
- Settlement:
  - $2.3 million and corrective action plan with 2 years of monitoring.

Lessons Learned from CHSPSC

- Access Controls, 45 C.F.R. §§ 164.310(a)(1), 164.312(a):
  - Facility
  - Electronic systems
- Security Incident Procedures, 45 C.F.R. § 164.308(a)(6):
  - Identify and respond to security incidents.
  - Mitigate harmful effects.
  - Document incident and outcome.

Athens Orthopedic Clinic PA

- September 21, 2020:
  - A hacker used a vendor's credentials to access a clinic's system and exfiltrate PHI of 208,557 patients.
  - OCR investigated and found that the clinic:
    - Had a longstanding and systemic noncompliance with the HIPAA rules.
    - Failed to conduct a risk analysis.
    - Failed to implement risk management.
    - Failed to implement audit controls.
    - Failed to maintain policies and procedures.
    - Failed to enter into required business associate agreements.
    - Failed to provide training to members of the workforce.
- Settlement:
  - $1.5 million and corrective action plan with 2 years of monitoring.

Lessons Learned from Athens Orthopedic

- Audit Controls, 45 C.F.R. § 164.312(b):
  - Hardware, software, and/or procedural mechanisms.
  - Record and examine activity in information systems.
- Training, 45 C.F.R. §§ 164.308(a)(5), 164.530(b):
  - Training required:
    - Within reasonable time after person is hired.
    - When the employee's job functions are affected by a change in privacy and security policies and procedures.
  - Training must be documented.
  - Ongoing security awareness training.

Lifespan Health System

- July 27,2020:
  - The laptop of a hospital's employee was stolen.
  - The laptop contained PHI of 20,431 individuals.
  - OCR investigated and found that the health system:
    - Failed to encrypt ePHI on laptops after Lifespan determined that encryption was reasonable and appropriate.
    - Failed to implement device and media controls.
    - Failed to have a business associate agreement with parent company.
- Settlement:
  - $1,040,000 and corrective action plan with 2 years of monitoring.

Lessons Learned from Lifespan

- *"Laptops, cell phones, and other mobile devices are stolen everyday, that's the hard reality. Covered entities can best protect their patients' data by encrypting mobile devices to thwart identity thieves."* –Roger Severino, OCR Director
- Device and Media Controls, 45 C.F.R. § 164.310(d)(1):
  - Govern receipt, removal, and movement of hardware and electronic media.
  - Address final disposition of ePHI and the associated hardware and media.
  - Record movements of hardware and electronic media.
  - Ensure backup of ePHI before movement of equipment.
- Encryption, 45 C.F.R. §§ 164.312(a)(1), 164.312(e)(1):
  - Encrypt ePHI at rest and in transit.
  - Understand limits of encryption (e.g., laptop with full disk encryption).
- Business Associate Agreements, 45 C.F.R. §§ 160.103, 164.308(b), 164.314(a):
  - A related entity can qualify as a business associate.
  - An agreement must be in place with all business associates.

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 disputes, 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 Hospitals

- 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.

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 $3,000,000.00 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

- Nov. 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.

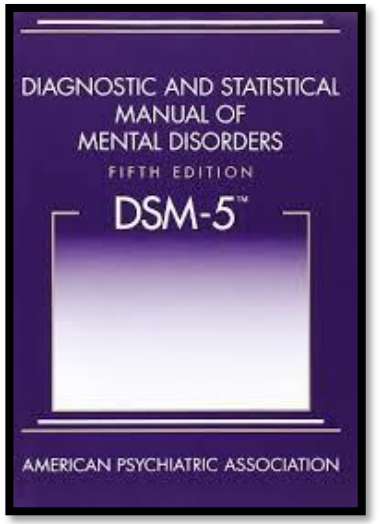
- October 15, 2018:
  - Largest U.S. health data breach.
  - $16 million settlement.
  - 79 million individuals affected.
  - Spear phishing.

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

- Mar. 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

Questions?

ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

Thank you!

Beth Anne Jackson, J.D.
Brown & Fortunato, P.C.
905 S. Fillmore, Ste. 400
Amarillo, TX 79101
bjackson@bf-law.com
806-345-6346

Allison D. Shelton, J.D.
Brown & Fortunato, P.C.
905 S. Fillmore, Ste. 400
Amarillo, TX 79101
ashelton@bf-law.com
806-345-6338

Board Certified, Health Law | Texas Board of Legal Specialization

BROWN & FORTUNATO
Celebrating 25 Years Together

ACHCU IS A BRAND OF ACCREDITATION COMMISSION *for* HEALTH CARE

ACHC®

Resources

- Unity Health to Pay $2.8M+ in Proposed Settlement over Phishing Attacks: Fox v. Iowa Health Sys., 3:18-cv-00327-JDP, Doc. Nos. 79 and 85-1
- 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