What's New In Healthcare Law?

Denise Burke, Esq.
Waller Lansden Dortch & Davis, LLP
1715 Aaron Brenner Drive, Suite 300
Memphis, TN 38120
901-288-1661
Denise.Burke@wallerlaw.com

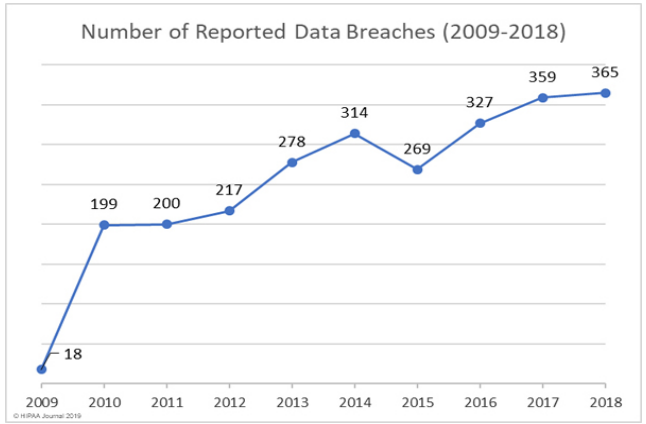
GOOD NEWS! OCR Lowers HIPAA Penalty Structure

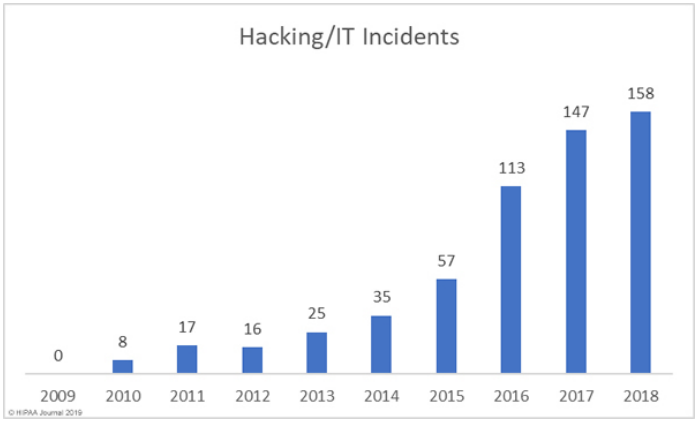
Previously $1.5 million cap for all Tiers

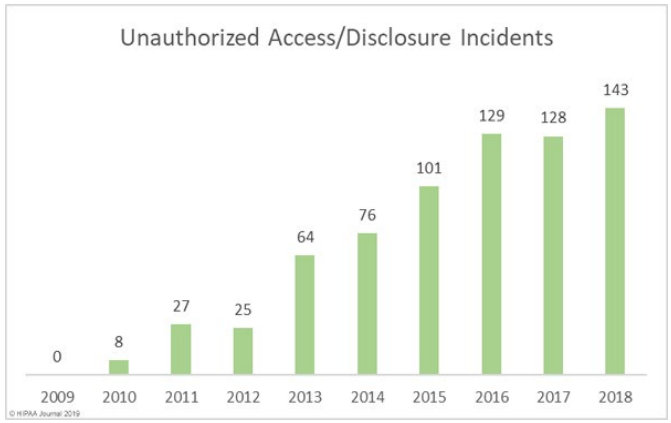
- Tier 1 (no knowledge of violation): $100 to $50,000 per violation; capped at $25,000 per year
- Tier 2 (reasonable cause): $1,000 to $50,000 per violation; capped at $100,000 per year
- Tier 3 (willful neglect, corrected): $10,000 to $50,000 per violation; capped at $250,00 per year
- Tier 4 (willful neglect, not corrected): $50,000 per violation; capped at $1.5 million per year

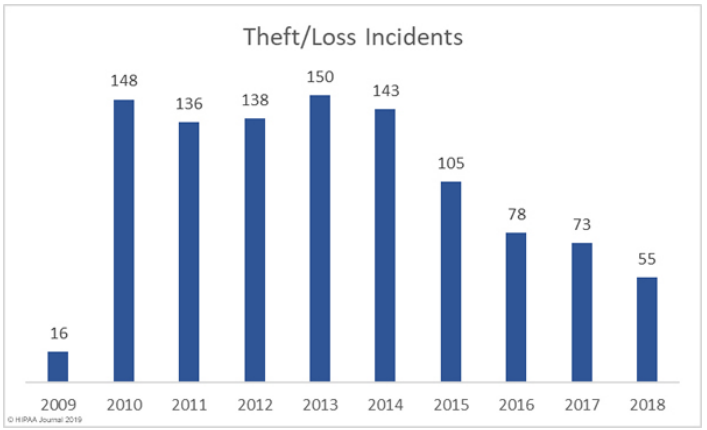
HIPPA Breaches Reported

- 2009 to 2018: 2077 500+ breaches reported









https://www.hipaajournal.com/healthcare-data-breach-statistics/

waller

Communicate, Educate and Remind Employees of Policies

Boston Medical Center, Brigham and Women's Hospital, and Massachusetts General

- In 2015, three independent hospitals permitted ABC to film documentaries without patient authorization
- In September 2018, each agreed to a settlement and CAP
- CAP:
  - "All members of BMC's workforce who have access to PHI have access to BMC's policy and procedure website, which includes BMC's policy on filming patients for non-clinical purposes, such as by the news media. BMC requires all workforce members to be familiar with and follow the policies and procedures on the policy and procedure website."
  - BMC will send an e-mail communication to all of its workforce members reminding them of BMC's policy on filming patients for non-clinical purposes. This email will include attachment of HHS' frequently asked question entitled, "Can health care providers invite or arrange for members of the media, including film crews. to enter treatment areas of their facilities without prior authorization'?"

Pagosa Springs Medical Center Lesson: Identify Business Associates, Enter Into BAAs And Implement A BAA Management Process

- In November 2018, Pagosa agreed to a settlement of $111,400 and corrective action plan arising from access by a former employee and disclosure to Google without a BAA.
- This creates 2 violations: no BAA and unauthorized access, use or disclosure
- Doubles the penalty
- GoogleDocs needs to know you are a healthcare provider

MD Anderson Lesson
Implement Encryption and Follow Through on Policies

- In October 2018, a $4.3 million civil money penalty was entered against MD Anderson based on the hospitals failure to implement encryption on laptops, USB drives and other devices despite a policy requiring encryption.
- “OCR is serious about protecting health information privacy and will pursue litigation, if necessary, to hold entities responsible for HIPAA violations,” said OCR Director Roger Severino. “We are pleased that the judge upheld our imposition of penalties because it underscores the risks entities take if they fail to implement effective safeguards, such as data encryption, when required to protect sensitive patient information.”
- MD Anderson policies and risk assessment identified the need for encryption of laptops and USB drives.

Fresenius Medical Care North America Lesson: Cumulative Small Breaches May Trigger An Investigation

- In January 2018, paid $3.5 million and agreed to a corrective action plan related to 5 breaches at separate locations – each affecting less than 500 individuals
- FMNCA failed to conduct a comprehensive enterprise wide security risk analysis of all of its ePHI
- Locations failed to implement appropriate security safeguards, including encryption

Cottage Health Lesson: Don't Forget To Include Changes In EnvironmentCottage

- In December 2018, CH agreed to a settlement of $3 million and corrective action plan arising from security vulnerabilities that left patient information accessible over the internet
- CH failed to conduct an accurate and thorough risk analysis, implement security measures, and perform a technical evaluation of newly installed Windows OS.
- CAP: In addition to performing a comprehensive security risk analysis, CH must "review the Risk Analysis annually," "promptly update the Risk Analysis in response to environmental or operational changes," and "assess whether its existing security measures are sufficient to protect its ePHI, and revise its Risk Management Plan, policies and procedures, and training materials."
- Also, "develop an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities identified in the Risk Analysis"

Conducting an SRA is just ½ of the process; management is the second ½.

Anthem, Inc. Lesson: Conduct and review information activity audits and train to prevent phishing attacks

- Response of at least 1 employee to a spear phishing attacks opened the door for an advanced persistent threat attack on the IT system; breach of 78.8 million
- In October 2018, Anthem agreed to pay $16 million and enter into a corrective action plan
- Costs to Anthem over $280 million, including OCR settlement "The largest health data breach in U.S. history fully merits the largest HIPAA settlement in history," said OCR Director Roger Severino. "Unfortunately, Anthem failed to implement appropriate measures for detecting hackers who had gained access to their system to harvest passwords and steal people's private information." Director Severino continued, "We know that large health care entities are attractive targets for hackers, which is why they are expected to have strong password policies and to monitor and respond to security incidents in a timely fashion or risk enforcement by OCR."

http://www.insurance.ca.gov/0400-news/0100-press-releases/2016/upload/Fully-Executed-RSA-2.PDF

Allergy Associates Lesson: Cross-Regulatory Referrals

- Investigation of discrimination complaint identified unauthorized disclosure to press
- OCR cross-regulatory investigations or inter-agency referrals
- Allergy Associates of Hartford agreed to a settlement of $125,000 and corrective action when a physician disclosed patient information to a reporter *in reckless disregard of counsel by privacy officer* not to discuss patient information with the reporter.

Start with Comprehensive Policies and Procedures

- All of the 2018 Resolution Agreements and Corrective Action Plans identified insufficient policies and procedures
- Comparing current policies against OCR Audit protocols is a helpful assessment
- OCR expects robust and specific policies
- Use of templates is considered a "red-flag"
- Make policies available to all staff
- Maintain revision history for 6 years
- Formal adoption by the Board or Compliance Committee is recommended
- Handle Breach Reporting Promptly

Resources

- HHS HIPAA for Professionals landing page with links to Regulations and Final Rules located at https://www.hhs.gov/hipaa/for-professionals/index.html
- 2018 OCR HIPAA Summary: Settlements and Judgments available at https://www.hhs.gov/sites/default/files/2018-ocr-hipaa-summary.pdf
- OCR Resolution Agreements available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
- OCR Audit Protocol available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
- Cybersecurity Act of 2015, Section 405(d):Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients available at https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
- OCR Cybersecurity Newsletters available at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html
- OCR Breach Notification Cases Under Investigation and archives available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- OCR Privacy, Security and Breach Notification Compliance Reports to Congress available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html
- OCR HIPAA New Releases available at https://www.hhs.gov/hipaa/newsroom/index.html
- NIST/OCR Safeguarding Health Information: Building Assurance through HIPAA Security -2018 with OCR and NIST materials available in links included in the Agenda at https://www.nist.gov/news-events/events/2018/10/safeguarding-health-information-building-assurance-through-hipaa-security
- Code of Alabama 1975, Section 8-38-1, et seq. available at http://alisondb.legislature.state.al.us/alison/codeofalabama/1975/coatoc.htm
- National Conference of State Legislation, Security Breach Notification Laws available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) available at https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/
- EU General Data Protection Regulation (GDPR) available at https://eugdpr.org/

MORE GOOD NEWS! Potential Stark Law Changes

AHA has recommended:

- Protection for value-based payment methodologies
- Clear, authoritative, and timely guidance
- Refocus regulations on arrangements that produce overutilization
- Eliminate requirement of compliance with Anti-Kickback Statute

CMS has hinted changes to come…

https://www.aha.org/letter/2018-08-03-aha-responds-cmss-rfi-reducing-regulatory-burden-stark-law

Eliminating Kickbacks in Recovery Act of 2018 (EKRA): October 24, 2018

A crime to knowingly and willfully:

- Solicit or receive any remuneration in return for referring a patient to a recovery home, clinical treatment facility, or laboratory; or
- Pay or offer any remuneration either to induce such a referral or in exchange for an individual using the services of a recovery home, clinical treatment facility, or laboratory.

Eliminating Kickbacks in Recovery Act of 2018 (EKRA): October 24, 2018

- Applies to laboratories even if the referral does not involve addiction treatment or recovery services
- "[C]linical treatment facility" includes any non-hospital entity that "provides detoxification, risk reduction, outpatient treatment and care, residential treatment, or rehabilitation for substance use"

Evaluate arrangements with all referral sources for private-pay patients to ensure that they do not involve any exchange of remuneration in exchange for patient referrals.

https://www.americanbar.org/groups/health_law/publications/aba_health_esource/2018-2019/march/ekra/

Eliminating Kickbacks in Recovery Act of 2018 (EKRA): October 24, 2018

- Applies to ALL Payors
- Only seven exceptions apply
- Penalties:
  - A fine of up to $200,000 per violation, and/or
  - Imprisonment for up to 10 years

New DOJ Compliance Guidance on Compliance (April, 2019)

- What Does the DOJ value in a Compliance Program

- "Is the corporation's compliance program well designed?"

- "Is the program being applied earnestly and in good faith?"
  - In other words, is the program being implemented effectively?

- "Does the corporation's compliance program work" in practice?

DOJ Compliance Guidance

- Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction in a low-risk area
- Credit for "revisions to corporate compliance programs in light of lessons learned."

- *https://www.justice.gov/criminal-fraud/page/file/937501/download*

DOJ Compliance Guidance

Policies and Procedures

- Design
- Comprehensiveness
- Accessibility
- Responsibility for Operational Integration
  - Have they been rolled out in a way that ensures employee's understanding of the policies?
- Gatekeepers
  - Do they know what misconduct to look for?
  - Do they know when and how to escalate concerns?

DOJ Compliance Guidance

Training and Communication

- Risk-Based Training
  - Has the company provided tailored training for risks in the area where the misconduct occurred?
  - Have supervisory employees received different or supplementary training?
  - How has the company measured the effectiveness of the training?
  - Have employees been tested on what they have learned?
- Communications about Misconduct
- Availability of Guidance

DOJ Compliance Guidance

Confidential Reporting Structure and Investigation Process

- Effectiveness of the Reporting Mechanism
  - Anonymous reporting mechanism?
  - How is the reporting mechanism publicized?
  - Has it been used?
- Properly Scoped Investigations by Qualified Personnel
  - What steps does the company take to ensure investigations are *independent, objective appropriately conducted*, and properly documented?
- Investigation Response
- Resources and Tracking of Results

DOJ Compliance Guidance

Is the Corporation's Compliance Program Being Implemented Effectively?

- Commitment by Senior and Middle Management
- Tone at the Top
- Oversight
  - What compliance expertise has been available to the **Board of Directors**?

DOJ Compliance Guidance

Autonomy and Resources

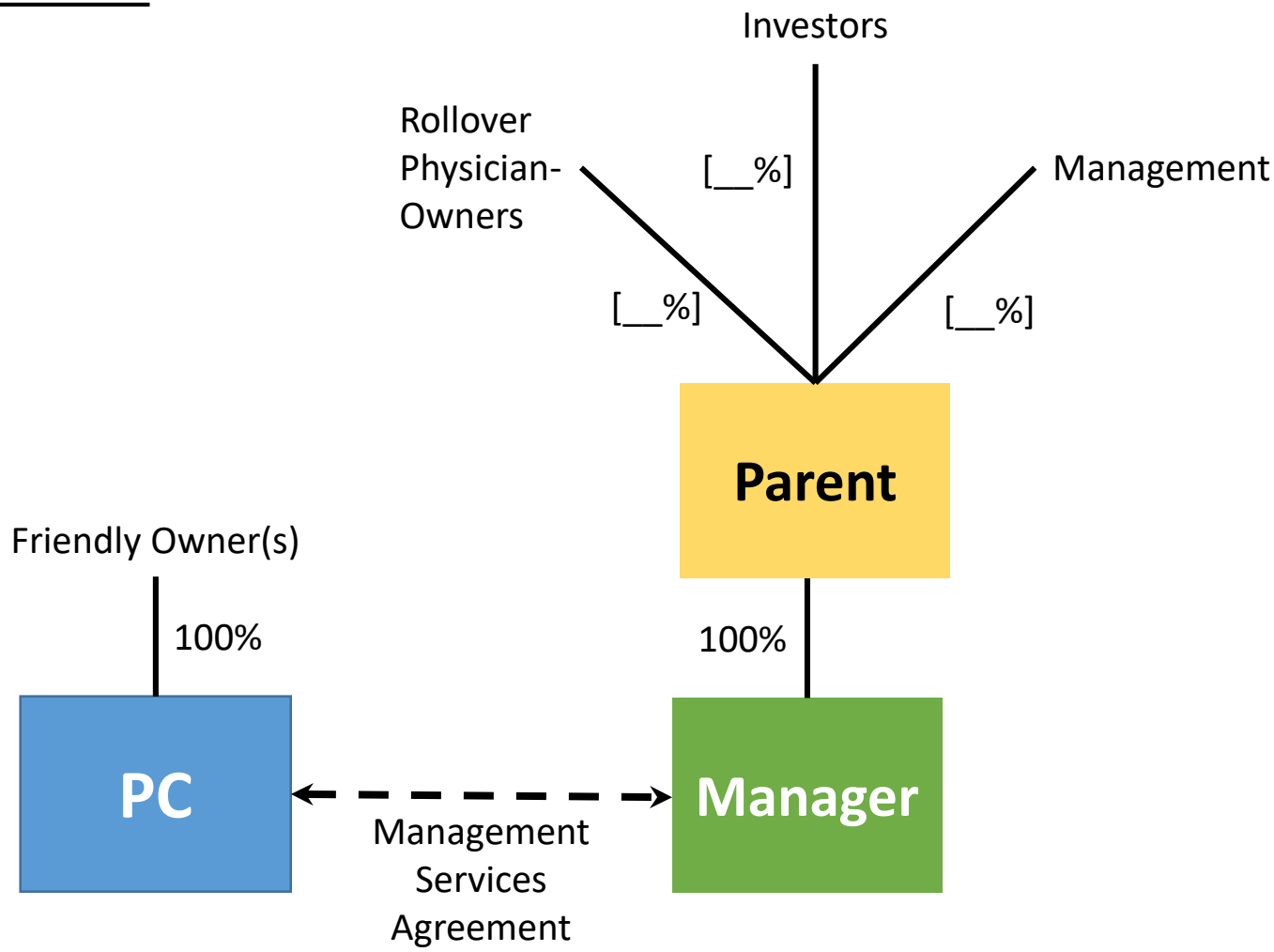
- Structure
  - Where within the company is the compliance function housed?
- Seniority and Statute
- Experience and Qualifications
- Funding and Resources
- Autonomy

CMS Draft Guidance on Hospital Co-location (May 3, 2019)

- Allows sharing public areas such as entrances, corridors through non-clinical areas and waiting rooms may be allowed
- Allows shared spaces such as public lobbies, staff lounges, elevators, corridors through non-clinical areas, restrooms, and main entrances
- Waiting rooms and reception areas can be shared as long as the areas are separate and clearly defined (own reception desks and the signage clearly notes the provider)
- Sharing of clinical space should be avoided
- No shared data unless access is needed for care
- Allows sharing of staff may be permissible, but not concurrent

Physicians and Private Equity

ROLLOVER MODEL



QUESTIONS?

Denise D. Burke

denise.burke@wallerlaw.com

(901)288-1651