DORSEY™
always ahead

HIPAA Enforcement and Settlements

Alissa Smith, Partner
Dorsey & Whitney LLP
Des Moines, IA

Objectives

- Describe HIPAA's Enforcement Rule
- Review numerous government enforcement actions under HIPAA
- Review internal responses to potential privacy violations
- Discuss responses to potential breaches and government inquiries

Outline of Presentation

- HIPAA enforcement rule
  - Definition and history
    - HIPAA and HITECH
- Enforcement agencies involved; Penalties; Process
- Enforcement statistics
- Enforcement examples, including:
  - Analysis of mitigating and aggravating factors
  - Resolutions and Civil Money Penalties
  - State cases; class actions
  - Lessons learned
- Internal responses to potential breaches
- Responding to government inquiries

Overview of Four HIPAA Rules

- The Privacy Rule: addresses the Use and Disclosure of PHI by Covered Entities and Business Associates and establishes individuals' privacy rights to understand and control how their health information is used.
- The Security Rule: establishes requirements for protecting electronic PHI (administrative, technical and physical safeguards).
- The Breach Notification Rule: requires notification to HHS, the individual and potentially the media following a Breach of Unsecured PHI.
- **The Enforcement Rule: establishes both civil money penalties ("CMPs") and federal criminal penalties, as well as procedures for agency enforcement and factors for assessing CMPs.**

HIPAA Violations and the Enforcement Rule

- **HIPAA violations occur when a covered entity (CE) or a CE's business associate (BA) fails to comply with any of the provisions of the HIPAA Privacy, Security, or Breach Notification Rules.**
  - **May be intentional or unintentional**
  - **Most violations are due to negligence/unintentional**
    - **Minimum Necessary Rule (limits the amount of information that be access, used, disclosed or requested)**
    - **Reasonable Safeguards Rule (requires reasonable administrative, technical and physical safeguards)**
    - **Results from failure to perform risk assessments and implement reasonable and appropriate risk mitigation**
    - **Lack of patient access to their PHI**

HIPAA Enforcement Agencies

- The Office of Civil Rights (OCR), housed within the Department of Health and Human Services (DHHS), is primarily responsible for interpretation and enforcement of HIPAA's Privacy, Security and Breach Notification Rules
- The Department of Justice (DOJ) becomes involved in criminal enforcement of HIPAA
- The Federal Bureau of Investigation (FBI) can become involved to help with investigation in some cases.
- State Attorneys General (SAG) are also empowered to bring civil actions on behalf of state residents for violations of HIPAA's Privacy and Security Rules (can obtain damages on behalf of residents or enjoin further violations).
  - OCR developed HIPAA Enforcement Training to help SAGs and their staff use their new authority to enforce the HIPAA Privacy and Security Rules.

The Enforcement Rule's History

- **Privacy Rule became effective in April, 2003 (Security Rule in April, 2005)**
- **Initially, investigations were infrequent, and fines were low and rare**
- **In 2009, it was determined that HIPAA could not account for the "revolution in information technology [which] encouraged a movement towards computerization of the storage and transmission of medical information."**
- **Therefore, the Department of Health and Human Services (HHS) decided to strengthen HIPAA and its enforcement capabilities through the Health Information Technology for Economic and Clinical Health (HITECH) Act**
- **HITECH allowed for the modification of the HHS Secretary's authority to impose CMPs for violations occurring after February 10, 2009.**

Office of Civil Rights Penalties

- Prior to HITECH, the HHS Secretary was only able to impose CMPs no greater of $100 for each violation or $25,000 for all identical violations of the same provision.
- Section 13410(d) of HITECH strengthened the Secretary's CMP authority by establishing a tiered penalty scheme ranging with increasing minimum penalty amounts, with a maximum penalty of $1.5 million for all violations of an identical provision.
- Under HITECH, almost all affirmative defenses were removed:
  - If not due to "willful neglect" and corrected within 30 days of discovery.
  - If criminal penalty imposed, no CMP may be imposed for same act

(Previously, affirmative defenses were available if CE did not have knowledge of the violation (and exercising reasonable diligence would not have had knowledge); or it was due to reasonable cause and not willful neglect and it was corrected within 30 days)

OCR Enforcement Perspective

- Every year, the number of violations and the amount of the settlements and civil money penalties are increasing (>$4M in 2012; >$6.5M in 2013; doubled each year thereafter- >$19M in 2017)
- Enforcement activities funded by settlements
  - 2018 budget for OCR decreased by $6M, but OCR said "not significant" because they will increase use of funds from settlements
- Current OCR Director, Roger Severino, has stated that the OCR will maintain the same programmatic focus as under the Obama Administration
  - HIPAA was a bipartisan law
  - with the revenue being brought in from the audit process, can recoup losses for meaningful use, Medicaid and Medicare
  - "…I expect we are going to see large monetary settlements for a long time to come…"

CMP Amount Considerations

- **The following are considerations in determining the amount of a CMP:**
  - **Nature of the violation**
    - **Number of individuals affected**
    - **Time period during which the violation occurred**
  - **Nature and extant of harm of violation**
    - **If the violation caused physical harm**
    - **If the violation caused financial harm**
    - **If the violation caused damage to individuals' reputations**
    - **If the violation impeded individuals' ability to obtain health care**
  - **Prior compliance history (of both the CE and BAs)**
    - **If the current violation appears similar to past indications of noncompliance**
    - **If the CE/BA has attempted to correct previous indications of noncompliance**
    - **If the CE/BA has responded to technical assistance from the Secretary and to what extent**
    - **How CE/BA has responded to past complaints**
  - **The financials of the CE/BAs**
    - **If the CE/BA has had previous financial difficulties that affected the ability to comply**
    - **If the CMP will jeopardize the CE/BA's ability to provide/pay for health care**
    - **The size of the CE/BA**

OCR's CMP Tier System

HIPAA Violation	Minimum Penalty	Maximum Penalty
Unknowingly (and by exercising reasonable diligence would not have known)	$100 per violation	$50,000 per violation, with an annual maximum of $1.5 million for identical violations
Reasonable Cause and not willful neglect	$1,000 per violation	$50,000 per violation, with an annual maximum of $1.5 million for identical violations
Willful neglect but violation is corrected within 30 days of the date the CE/BA knew (or by exercising reasonable diligence would have known)	$10,000 per violation	$50,000 per violation, with an annual maximum of $1.5 million for identical violations
Willful neglect and is not corrected within 30 days of the date the CE/BA knew (or by exercising reasonable diligence would have known)	$50,000 per violation	Annual maximum of $1.5 million for identical violations

HIPAA Criminal Enforcement

- **In order for the DOJ to seek criminal penalties, the CE, BA, or individual(s) within either, must be found to have "knowingly" obtained or disclosed PHI**

In a Memorandum Opinion from the DOJ entitled, "Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6" the DOJ answered the following question from HHS:

"[HHS] asked whether the 'knowingly' element of section 1320d-6 requires only proof of knowledge of the facts that constitute the offense or whether this element also requires proof of knowledge that the conduct was contrary to the statute or regulations."

The DOJ concluded, "that 'knowingly' refers only to the knowledge of the facts constitute the offense."

HIPAA Criminal Enforcement

- **Additionally, DOJ answered the following question from HHS:**
  - **"[HHS] asked…whether the only persons who may be held directly liable under [the] section…are those persons to whom the substantive requirements of the subtitle, as set forth in the regulations…or whether this provision may also render directly liable persons…who obtain [PHI] in a manner that causes a person…to release the information in violation of that law."**
  - **The DOJ determined that CE/BAs "specified in the statute…may be prosecuted for violations…In addition, depending on the facts of a given case, certain directors, officers, and employees of these entities…in accordance with general principles of corporate criminal liability"**

Department of Justice Criminal Penalties

- **Much like the OCR civil penalties, the DOJ has tiered penalty scheme, including monetary fines and incarceration time**

HIPAA Violation	Fines	Jail Sentence
Unknowingly or with reasonable cause	Up to $50,000	Up to 1 year
Under false pretenses	Up to $100,000	Up to 5 years
For personal gain or malicious reasons	Up to $250,000	Up to 10 years

OCR Investigations

- **Result from:**
  - **Complaints**
  - **Breach Notifications**
  - **Audits**
  - **Compliance Reviews (if OCR has reason to believe there may be a violation- e.g., media reports)**
  - **Information received from other agencies (e.g., FBI)**

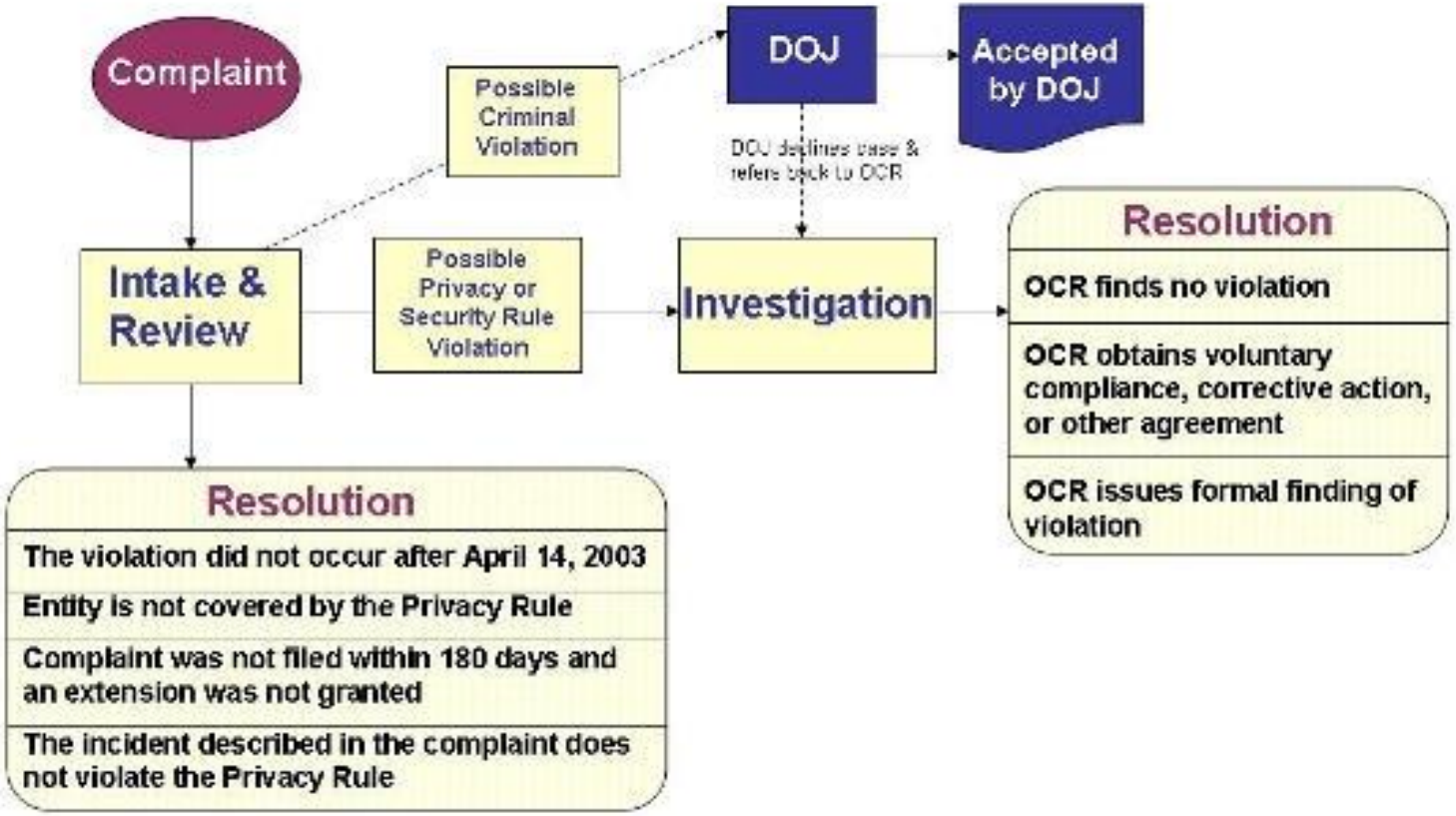
OCR Complaints

- **OCR investigates all complaints of potential HIPAA violations.**
- **Complaints are coming in at an all time high- as more patients become aware of their rights under HIPAA.**
- **200% increase since 2012 when OCR started a more efficient complaint intake process (on-line portal)**
- **In order for the OCR to take action on complaints, the following conditions must be met:**
  - **The compliant must be against a CE or BA that is required to comply with the Privacy and Security Rules**
  - **The compliant must be about an activity that would violate the Privacy or Security Rule**
  - **Complaints must be filed within 180 days of the alleged violation**

Office of Civil Rights Complaint Process

- If the complaint fits the criteria, OCR will take the following steps:
  - Notify the person who filed the complain as well as the CE/BA named in the complaint
    - Both parties present information about the alleged violating action/actions
      - CEs/BAs are required by law to cooperate with complaint investigations.
  - The information/evidence is reviewed.
  - If the evidence indicates that the CE/BA was not in compliance, the following actions take place:
    - Voluntary compliance/technical assistance;
    - Settlement negotiations with a corrective action plan; or
  - If a CE fails to take action to resolve the matter to the OCR's satisfaction, CMPs may be imposed
    - CMPs are deposited to the U.S. Treasury, not to the OCR/HHS
  - If a violation meets the criminal standards of HIPAA (42 U.S.C. 1320d-6), the OCR may refer the complaint to the Department of Justice (DOJ) for further investigation

HIPAA Privacy & Security Rule Complaint Process



Audits

- Prior to HITECH in 2009, audits were rare
- HITECH requires OCR to conduct periodic audits of CE and BA compliance with the HIPAA Privacy, Security, and Breach Notification Rules.
- In 2011 and 2012, OCR implemented a pilot audit program to assess the controls and processes implemented by 115 covered entities to comply with HIPAA's requirements.
  - Incomplete/not implemented risk analysis
  - Lack of customized policies and procedures
  - Lack of staff training
  - Lack of contingency plans
  - Lack of proper internal auditing
  - Lack of breach notification
  - Small providers worse than larger ones
  - Security Rule is the largest concern (65% of the deficiencies)
- OCR implemented phase two of the program in 2016, which audits both covered entities and business associates.

State Data Privacy and Breach Notification Laws

- **In addition to HIPAA, almost all states across the country have adopted various laws that require breach notification, privacy and confidentiality standards, and impose additional penalties.**
  - **E.g., Iowa Code 715C**
    - **Personal Information Security Breach**
      - **Only for computerized information breaches**
      - **Only for "personal information" which is first name or first initial + last name in combination with unencrypted/readable data elements: SSN, DLN or unique gov't ID, financial account of CC number + PIN or security code allowing access to account, unique biometric data like a fingerprint**
    - **Notification to the "consumer", and generally also to the AG**
    - **Separate penalties- unlawful practice under consumer fraud law, remedies available to the AG, and violator can be ordered to pay damages to the AG on behalf of injured person**

Personal Lawsuits

- **HIPAA does not provide for a private right of action for plaintiffs.**
- **Violations are subject only to enforcement actions by OCR or SAG on behalf of plaintiffs.**
- **BUT**
  - **Courts in some states have allowed plaintiffs to use HIPAA as a standard of care/legal duty in state law tort negligence actions against healthcare providers for privacy violations**
  - **Claims have included losses/injuries from slander/defamation, financial, reputational, negligent infliction of emotional distress**
  - **E.g.: Connecticut, New York, Massachusetts, Missouri, West Virginia, Tennessee, Minnesota, and North Carolina.**

Recent Personal Lawsuit Example

January 16, 2018- the Connecticut Supreme Court ruled in favor of Emily Byrne based on state law negligence and negligent infliction of emotional distress claims against Avery Center for Obstetrics and Gynecology in Westport, Connecticut. The Court ruled that HIPAA can inform the standard of care, creating a cause of action in tort for violations of the standards established by federal public policy.

- **Avery Center provided Byrne's medical records (pregnancy test) to the child's father in response to a subpoena issued in a paternity suit. However, instead of appearing in court, as required by the subpoena, Avery Center mailed a copy of Byrne's records to the New Haven Regional Children's Probate Court.**
- **HIPAA requires certain measures be taken to obtain satisfactory assurances regarding notice to the individual (with opportunity to object) or a protective order**

Class Action and State Action Example

- **January, 2018- Aetna settled a class action for $17M- based on two separate disclosures of member PHI in one of the largest data breaches involving HIV-related information**
- **Claims of privacy violations related to the disclosure of thousands of its health plan members' HIV status.**
  - **Allegations that in 2014 and 2015, Aetna improperly disclosed HIV status to legal counsel, a settlement administrator and a mailing vendor in connection with prior lawsuits**
  - **Second breach allegation was when Aetna exposed HIV-related information, including medication information, by mailing notification letters to members in envelopes with large, clear windows that exposed the information**
- **$17M goes into a fund to be distributed to the 11,875 members of one affected class, and the 1,600 members of the other class**
- **Aetna must develop and implement "best practices" policy for the use of its members' PHI. (e.g., opaque envelopes with no information on the outside regarding health information inside, include only minimum necessary information in the letter, mark it highly confidential on an internal seal, use paper stock that maintains privacy and can't be seen through envelope)**
- **Aetna also paid $1.15M to NY AG based on its investigation of these class action breaches that identified another mail-related privacy breach earlier the same year that had indications on the outside of the patient's health condition.**

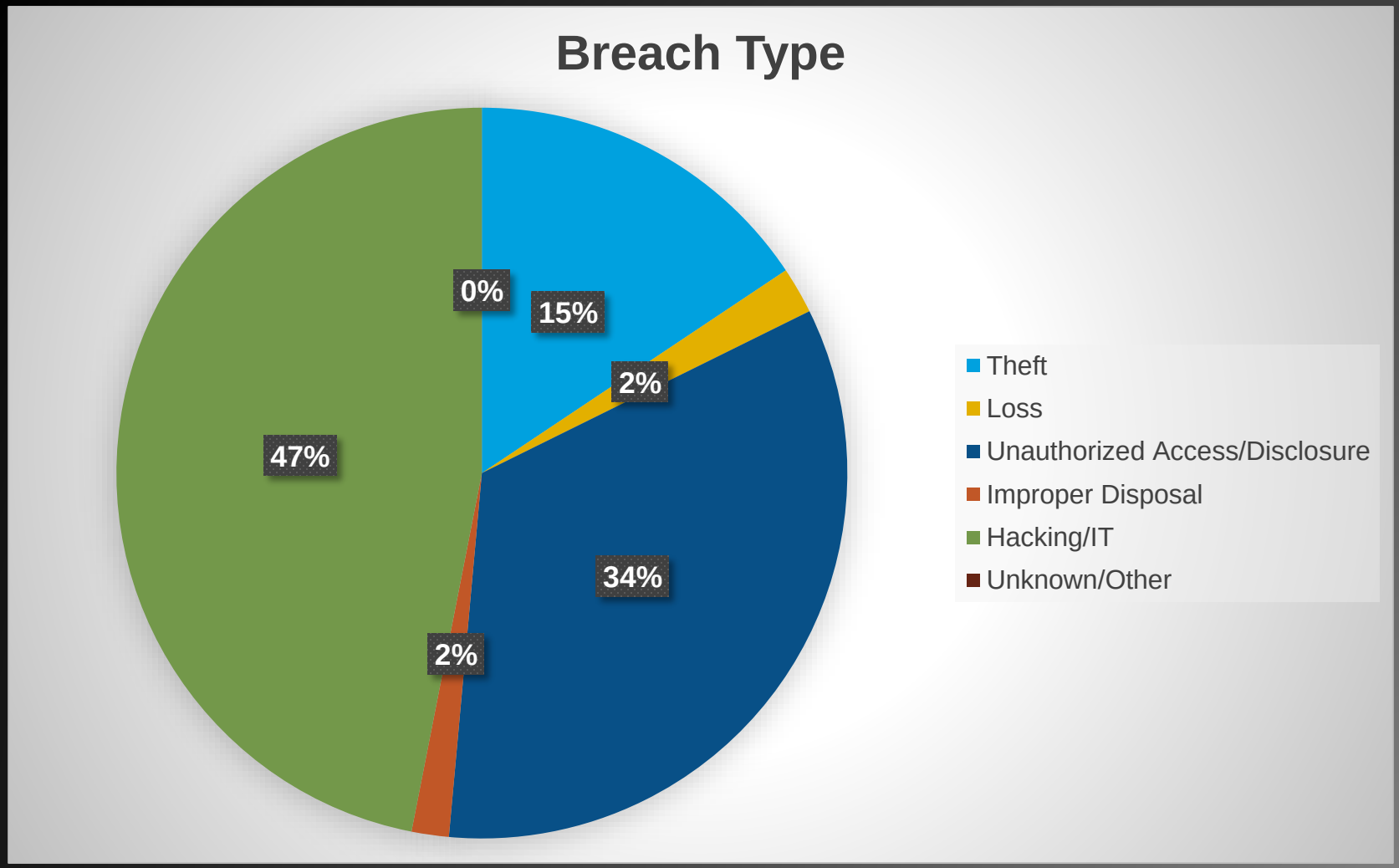
Statistics-2017

- Between April 2003-December 2017:
  - 171,161 HIPAA complaint cases/potential breaches have been reported to OCR
  - OCR Initiated over 850 compliance reviews on its own
  - OCR Resolved 164,252 complaint cases (98%)
    - Investigated/resolved 25,312 cases by requiring changes through corrective action or providing technical assistance
    - Referred 664 referrals to the DOJ for criminal sanctions
    - Reached settlements (called Resolution Agreements) with 53 entities since 2009, totaling $75,229,182.00
- Almost all Settlements include a 2 to 3-year corrective action plan
- Most settlements are a result of an initial breach notification

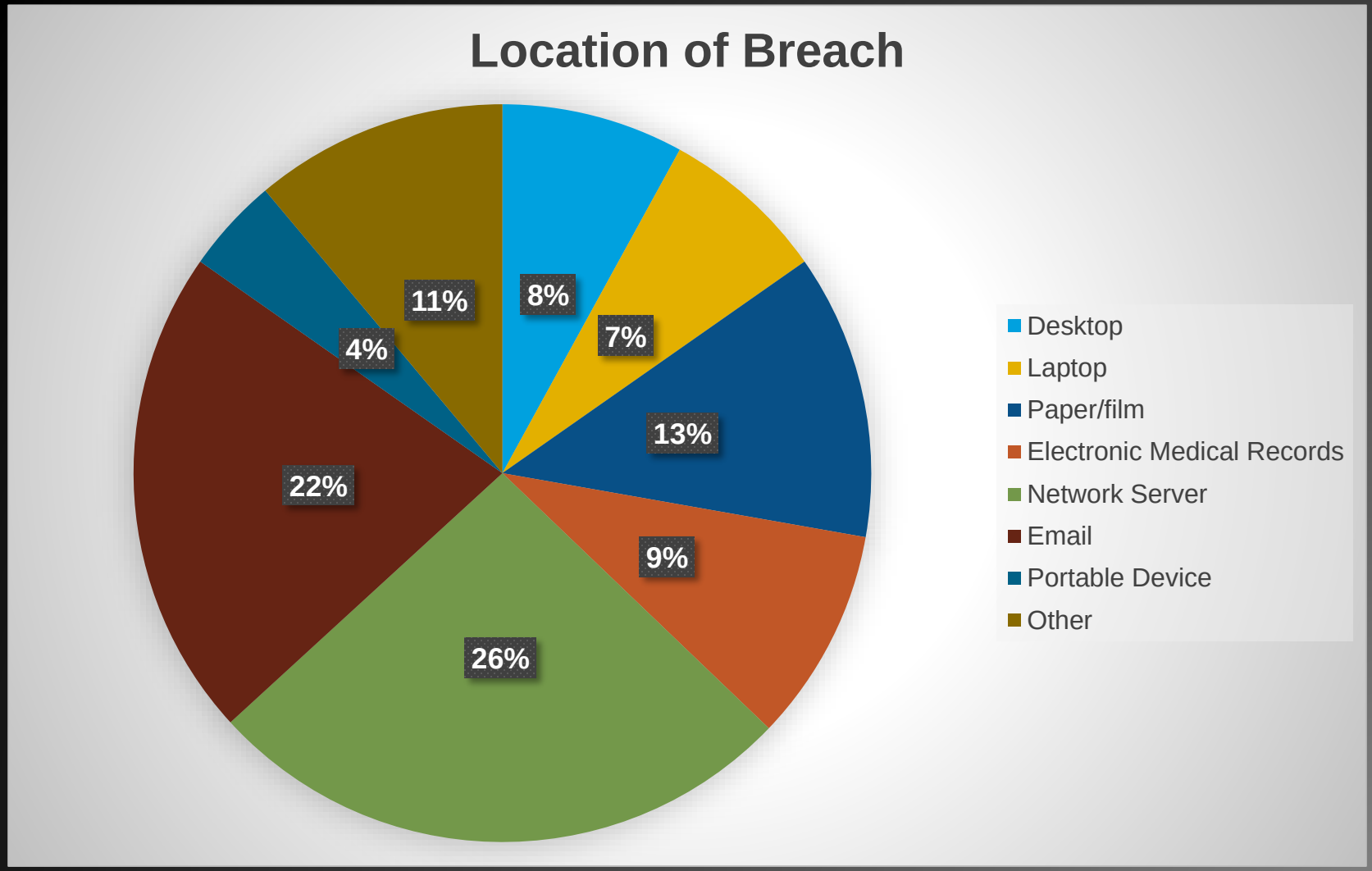
Current State of Affairs

- External threats at all time high
  - #1 problem resulting in a settlement is cyber hacking/ransomware attacks
- Internal threats are the largest source of risk for covered entities – loss of mobile devices, snooping, social media mistakes
  - #2 problem resulting in a settlement is loss/theft of unencrypted portable devices
- More individual complaints
- OCR enforcement posture more aggressive
- OCR widening review of small breaches (previously usually only investigated large breaches)
- Settlement amounts are increasing

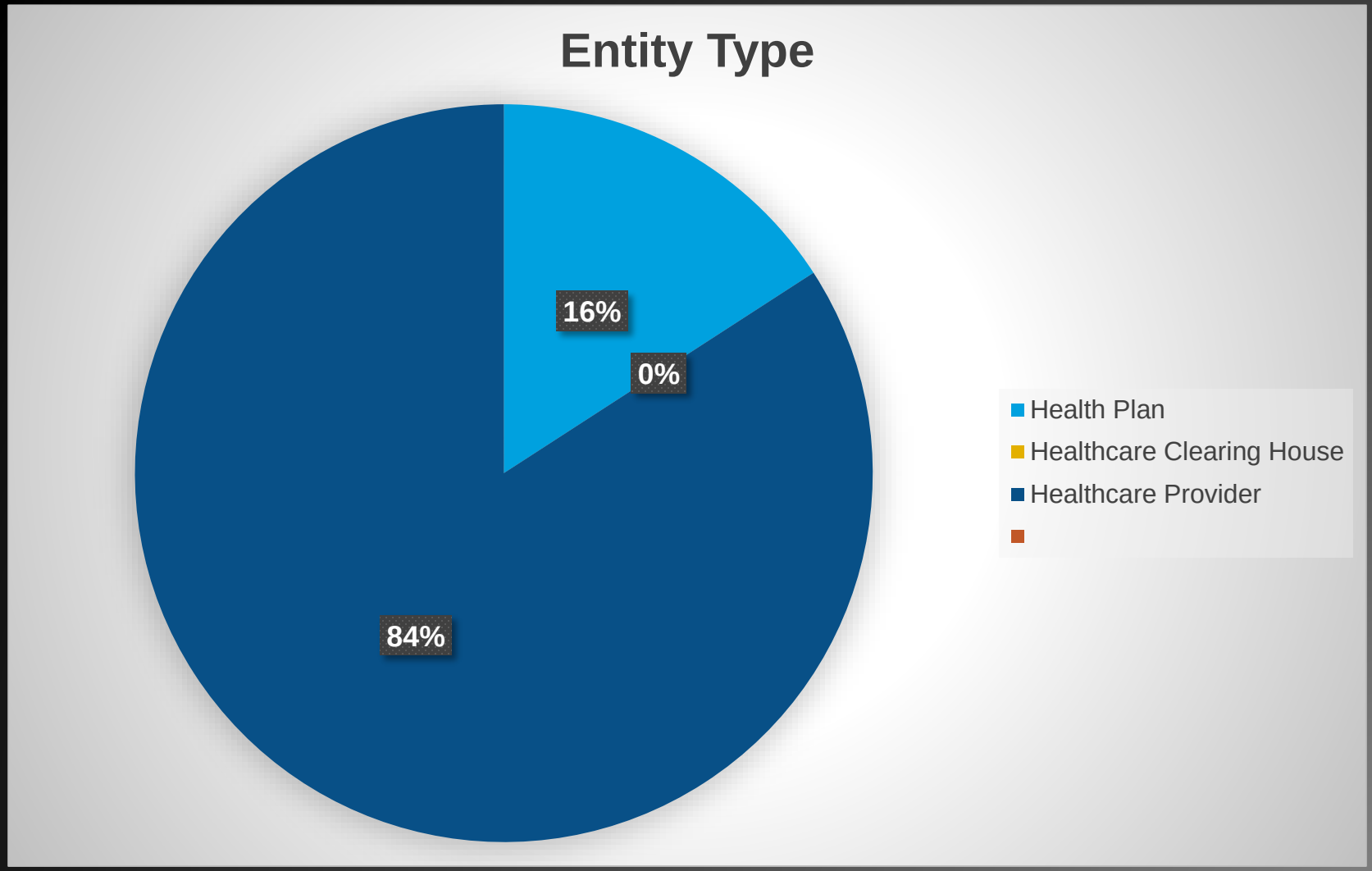
Statistics-2017 (continued)



Statistics-2017 (continued)



Statistics-2017 (continued)



Resolution Agreements (RAs) & Corrective Action Plans (CAPs) Example:

- **Children's Medical Center (hospital)-(filed 1/18/2010 AND 7/5/13; Feb., 2017)**
  - **2010 Breach: An unencrypted BlackBerry was reported lost at an airport**
    - **3,800 affected individuals**
  - **2013 Breach: an unencrypted laptop was reported stolen from hospital premises**
    - **2,462 affected individuals**
  - **Between the two incidences, the ORC determined that Children's was in violation of numerous HIPAA rules. After the 2010 incident, it failed to implement a risk management plan to avoid the 2013 breach. No encryption or alternative until 2013 for laptops, blackberries, other mobile devices. Also, it allowed non-authorized workforce members access to ePHI.**
  - **Total (CMP) amount: $3.2 million**

Resolution Agreements (RAs) & Corrective Action Plans (CAPs) Example:

- **Memorial Healthcare System (MHS)- Feb, 2017**
  - **Failed to terminate access of former employee, which had been used daily by this individual between April 2011 (termination date) and April 2012**
  - **Affecting up to 115,134 individuals**
  - **Despite this risk ID'd yearly from 2007-2012 in risk analysis, No regular audits of access/system activity, no access removal procedure upon termination**
  - **Resolution amount $5.5 million**
  - **Length of CAP: 3 years**
  - **CAP requirements**
    - **Completion of Risk Analysis and Risk Management Plan**
    - **Revision of Policies & Procedures**
    - **Adoption of Distribution of Policies & Procedures**
    - **Monitoring**
    - **Internal Reporting**
    - **Annual Reports**

Resolution Agreements (RAs) & Corrective Action Plans (CAPs) Example:

- **Metro Community Provider Network (a federally-qualified health center) (filed 1/27/12- resolution April, 2017)**
  - **Hacker accessed employees' email accounts through a phishing scam**
- **3,200 affected individuals**
- **OCR found no risk analysis or security risk management plan until 2012**
- **Resolution Agreement amount: $400,000 (taking into account status as an FQHC/financial ability to pay)**
- **Length of CAP: 3 years**
- **CAP requirements**
  - **Conduct Risks Analysis**
  - **Develop and Implement Risk Management Plan**
  - **Review and revise Policies and Procedures**
  - **Review and Revise Training Materials**
  - **Regular Reporting**

Resolution Agreements (RAs) & Corrective Action Plans (CAPs) Example:

- **Center for Children's Digestive Health (Settlement April, 2017)**
- **When OCR was investigating a BA of CCDH (File Fax- a records storage vendor who we will see again in this presentation), OCR discovered that the BA did not have a BAA with CCDH.**
- **OCR opened a "compliance review" of CCDH, and discovered that between 2003- 2015, no BAA was in place with FileFax.**
- **Resolution Agreement amount: $31,000**
- **Length of CAP: 2 years**

Resolution Agreements (RAs) & Corrective Action Plans (CAPs) Example:

- Memorial Hermann Health System (Settlement May 2017)
- Authorities alerted of a crime on the premises (medical ID theft)
- Alerting authorities was permitted under HIPAA. What happened next, was not.
- Management published press release including patient's name.
- OCR found no evidence of employee sanction for impermissible disclosure.
- Resolution Agreement amount: $2.4 million
- Length of CAP: 2 years

Resolution Agreements (RAs) & Corrective Action Plans (CAPs) Example:

- 21st Century Oncology, Inc. (21CO) (Settlement December 11, 2017)
- On two separate occasions, through the remote desktop protocol from an exchange server within 21OC's network, information (including patient names, social security numbers, physicians' names, diagnoses, treatment, and insurance information) was obtained by an unauthorized third party and produced to an FBI informant.
- OCR investigation revealed that 21CO had
  - Failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities of the ePHI
  - Failed to implement procedures to regularly review records of information system activity
  - Disclosed PHI to third party vendors without a written BA agreement
- Resolution Agreement amount: $2.3 million
- Length of CAP: 3 years
- Bankruptcy
  - In December 2017, the OCR accepted a settlement approved by the US Bankruptcy Court for the Southern District of New York
  - 21CO filed for Chapter 11 bankruptcy protection
    - CAP is still in place to ensure that the 21CO "emerges from bankruptcy with a strong HIPAA compliance program in place."

Resolution Agreements (RAs) & Corrective Action Plans (CAPs) Example:

- **Fresenius Medical Care North America (FMCNA) (Settlement February 1, 2018)**
- **Between February-July 2012, five separate breaches were reported in various Florida branches of FMCNA due to FMNCA:**
  - **Failing to perform accurate and thorough risk analysis.**
  - **Failing to implement policies and procedures to address security incidents**
  - **Disclosing ePHI by allowing access for a purpose "not permitted by the Privacy Rule"**
  - **Failing to implement a mechanism to encrypt and decrypt ePHI**
- **Resolution Agreement amount: $3.5 million**
- **Length of CAP: 2 years**

Resolution Agreements (RAs) & Corrective Action Plans (CAPs) Example:

- **Filefax (Settlement February 13, 2018)**
- **In January and February of 2015, 2,150 individuals' PHI was disclosed by leaving the information in an unlocked truck of the Filefax parking lot, as well as granting an unauthorized person access to the PHI**
- **Resolution Agreement amount: $100,000**
- **Filefax is no longer in business, however, remaining assets that have been liquidated to pay for the Resolution Agreement amount**
  - **On behalf of Filefax, a receiver has agreed to be the properly dispose of the remaining medical records.**

Lessons to Be Learned

- **The exposure of PHI can be technical (unencrypted devices) and non-technical (loss of papers/property containing PHI)- resources should be applied to prevent both**
- **There is no substitute for customized, implemented HIPAA policies and procedures, with frequent training of staff to mitigate risk from the inside**
- **Business grade IT security is critical to mitigate risk from outside threats**
- **Ongoing implementation of risk assessments is critical to update responses as business and technology evolves**
- **Screen and monitor BAs (there are more than 7M BAs in the US)**
- **Timely reporting to OCR is important**

Internal Responses to Potential Privacy Violations

- Analyze potential breaches in good faith. 45 CFR 400
- Hire counsel and consultants if needed to evaluate the issues
- Use breach response team to ensure multiple perspectives; follow breach response policies and protocol (e.g., forms, 2-person interviews, when to hired outside experts, attorney-client privilege considerations)
- Ensure a process is provided for individuals to make complaints regarding HIPAA. 45 CFR 164.530(d)
- Ensure appropriate sanctions are applied to workforce members who fail to comply. 45 CFR 164.530 (e)
- Do not intimidate or retaliate against any person who files a complaint, testifies or assists in an OCR investigation or proceeding, or who opposes any act or practice that is unlawful under HIPAA. 45 CFR 160.316
- Mitigate any harmful effects (to the extent practicable) (e.g., credit monitoring) 45 CFR 164.530 (e)
- Report all breaches timely in accordance with HIPAA's Breach Notification Rule. 45 CFR 400
- Report as required under applicable state law

Internal Responses to Potential Privacy Violations (cont'd)

- Review and update policies if needed to ensure non-compliance will not happen in the future (and to be prepared in the event of an investigation
- Retrain staff if needed to prevent non-compliance; prepare key staff about what to expect in the event of an investigation
  - Where are policies; who are internal privacy and security officers; what do policies say
- Have policies, procedures, risk assessments, security risk analysis, and other compliance documentation organized and ready in case of an investigation

Responses to Government Investigations

- Respond promptly
- Cooperate with investigation
- Don’t be defensive/surly
- Demonstrate commitment to HIPAA compliance at highest level

Questions?

Alissa Smith

Partner

Dorsey & Whitney, LLP

smith.alissa@dorsey.com

(515) 699-3267