


United States Department of
Health & Human Services

Current State of HIPAA Enforcement

Midwest Region
United States Department of Health and Human Services
Office for Civil Rights



Disclaimer

- These power point slides are intended to be purely informational and informal in nature. Nothing in the slides are intended to represent or reflect the official interpretation or position of the Department of Health and Human Services, the Office for Civil Rights.

1



Topics

- Overview of the Enforcement Process
- OCR HIPAA Enforcement Actions from 2013 to present
- Enforcement Statistics and Upcoming Enforcement Activities
- New OCR HIPAA Rules, Guidance, and Tools
- OCR Resources

2



HIPAA Enforcement Actions: Recent Cases and Trends

Security Rule and Privacy Rule Cases from 2013

3

Affinity Settles in Photocopier Security Rule Breach Case for \$1,215,780


- Affinity Health Plan impermissibly disclosed the protected health information of up to 344,579 individuals when it returned multiple photocopiers to a leasing agent without erasing the data contained on the copier hard drives.
- OCR's investigation revealed that Affinity failed to incorporate the electronic protected health information stored in copier's hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the hard drives to its leasing agents.
- The corrective action plan required Affinity to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased and that remained in the possession of the leasing agent, and to take certain measures to safeguard all ePHI.

4

WellPoint pays \$1.7 million for leaving information accessible over Internet

- WellPoint's breach report indicated that security weaknesses in an online application database left the electronic protected health information (ePHI) of 612,402 individuals accessible to unauthorized individuals over the Internet.
- OCR's investigation indicated that WellPoint did not implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule:
 - WellPoint did not adequately implement policies and procedures for authorizing access to the on-line application database.
 - Did not perform an appropriate technical evaluation in response to a software upgrade to its information systems.
 - Did not have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database.

5



Hospice of North Idaho, a Small Provider, Pays \$50,000 to Settle

- This was the first case involving a breach report for PHI of fewer than 500 individuals which resulted in the execution of a Resolution Agreement by the CE and the payment of a Resolution Amount to OCR, namely \$50,000.
- In 2010, Hospice of North Idaho (HONI) submitted a breach notification, reporting that a laptop containing the PHI of 441 patients had been stolen.
- OCR's investigation showed that HONI had not conducted a risk analysis and had not promulgated a policy designed to ensure the security of PHI held on mobile media devices.
- Since the breach was discovered, HONI did take substantial steps to improve its privacy and security compliance program.

6



Adult & Pediatric Dermatology Pays \$150,000 to Settle Breach Notification Case

- OCR received a report that an unencrypted thumb drive containing ePHI for 2200 individuals was stolen from a staffer's car.
- The thumb drive was never recovered.
- OCR investigation showed that APDerm had not conducted an analysis of risks and vulnerabilities regarding ePHI.
- APDerm did not have a written policy for reporting breaches and training employees on Privacy and Security Rule issues.

7

Shasta Regional Medical Center Settles Privacy Rule Case for \$275,000 for Impermissible Disclosure

- SRMC failed to safeguard the patient's protected health information (PHI) from impermissible disclosure by intentionally disclosing PHI to multiple media outlets on at least three separate occasions, without a valid written authorization.
- OCR's review indicated that senior management at SRMC impermissibly shared details about the patient's medical condition, diagnosis and treatment in an email to the entire workforce.
- In addition, SRMC failed to sanction its workforce members for impermissibly disclosing the patient's records pursuant to its internal sanctions policy.
- A corrective action plan (CAP) required SRMC to update its policies and procedures on safeguarding PHI from impermissible uses and disclosures and to train its workforce members.
- The CAP also required fifteen other hospitals or medical centers under the same ownership or operational control as SRMC to attest to their understanding of permissible uses and disclosures of PHI, including disclosures to the media.

8

Parkview Health Systems Settles for \$800,000

- Parkview, an Indiana entity, took custody of medical records for 5000 to 8000 patients from a retiring physician who wanted to transition her patients to new providers. Parkview was considering the possibility of purchasing a portion of the physician's practice.
- Subsequently, with notice that the physician would not be at home, Parkview left 71 bankers boxes of medical records unattended in the driveway of the physician's home within 20 feet of a public road and a short distance from a heavily trafficked public shopping venue.
- While transferring the records back to the retired physician, Parkview failed to take adequate steps to properly protect the PHI of the doctor's patients.

9



Community Health Centers Settle Security Rule Case

- The Anchorage Community Mental Health Services (ACMHS), a five-facility, nonprofit organization providing behavioral health services, reported a breach of unsecured e-PHI affecting 2743 individuals due to malware compromising the security of its IT resources.
- In its investigation, OCR determined that ACMHS had adopted sample Security Rule policies and procedures in 2005, but had not adhered to them. In addition, ACMHS had not done even a rudimentary risk analysis and had failed to update its IT resources with available patches. ACMHS had also used outdated, unsupported software.
- ACMHS paid a resolution amount of \$150,000, changed its policies and procedures, and agreed to submit reports to OCR for two years.

10



Cancer Care Group Settle Security Rule Case

- Cancer Care Group (CCG), a physicians practice with 13 radiation oncologists, reported a breach of unsecured e-PHI affecting 55,000 individuals as a result of a laptop bag being stolen from an employee's car. The bag contained unencrypted backup media tapes, which contained PHI.
- In its investigation, OCR determined that CCG was in widespread non-compliance with the HIPAA Security Rule. CCG had not done an enterprise-wide risk analysis nor did it have a policy specific to device and media control. In this case, the removal of hardware and electronic media containing e-PHI into and out of its facilities, although it was a common practice.
- CCG paid a resolution amount of \$750,000.

11



Lessons Learned

- The Privacy and Security Rule apply to all aspects of a covered entity's operations, including potential business expansion when other providers' records come into the covered entity's possession.
- Risk analysis have to be undertaken and the findings addressed.
- There is a duty to keep up with the technology, at least to the extent of using readily available patches and supportable software.
- Protecting paper PHI still matters.
- Train heavily and stringently implement security policies.
- ENCRYPT, ENCRYPT, ENCRYPT.


12



Lessons Learned


- HIPAA covered entities and their business associates are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information.
- Take caution when implementing changes to information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers' health data using the Internet.
- Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients' rights are fully protected.

13



Enforcement Statistics and Upcoming Enforcement Activities

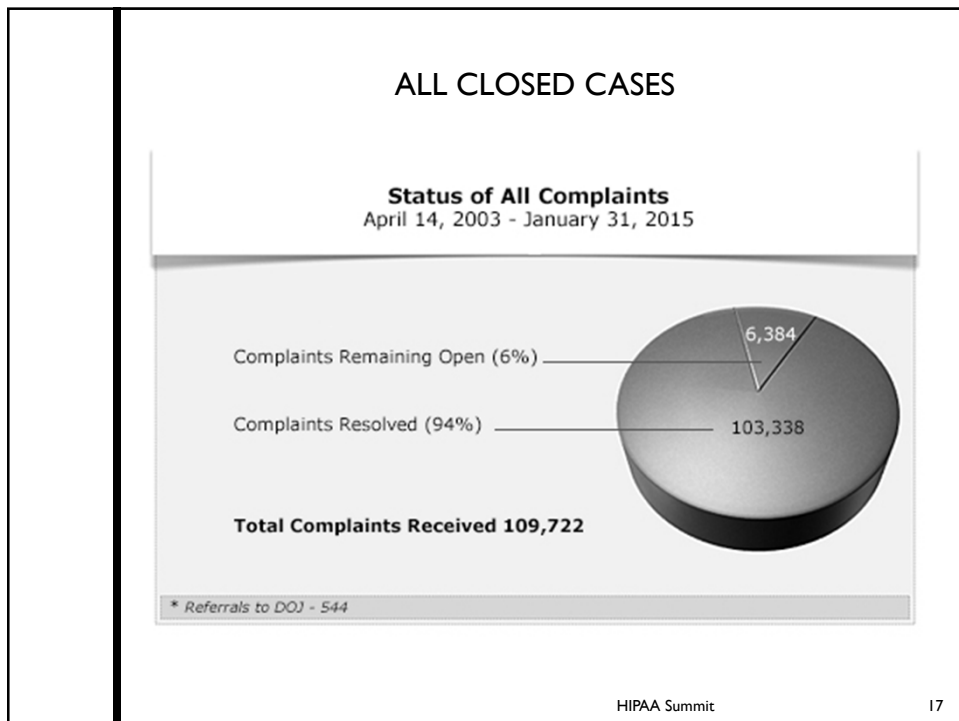
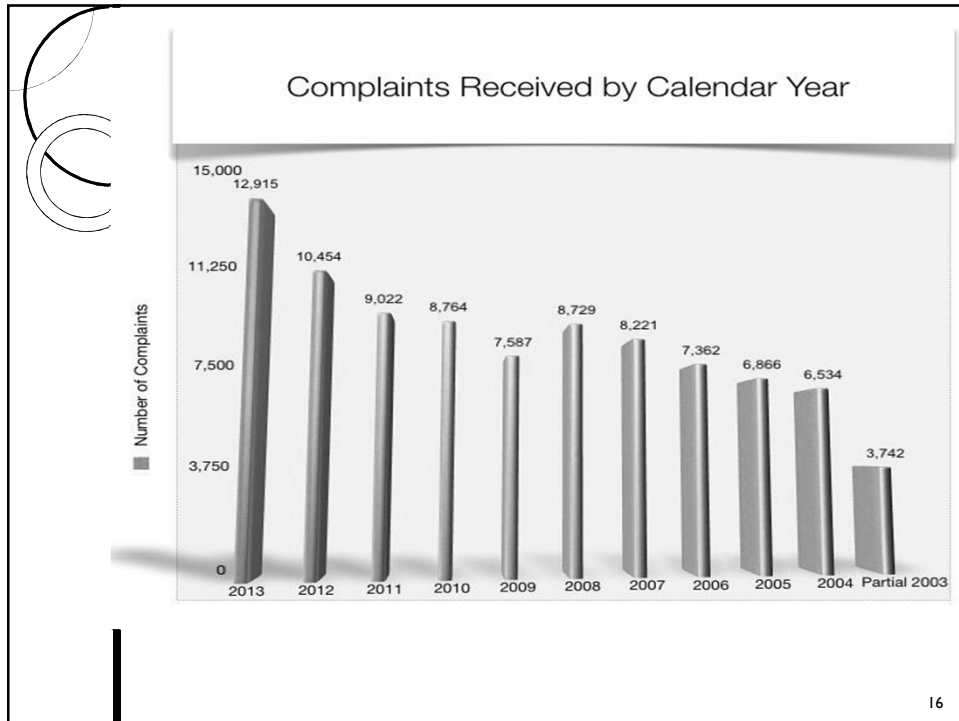
14



Top Five Issues Nationally in Cases Closed in 2013 with Corrective Action

1. Impermissible Uses and Disclosures of PHI
2. Lack of adequate physical, technical, or administrative safeguards
3. Individuals or their Representatives Being Denied Access to their PHI
4. Minimum Necessary
5. Lack of Mitigation by CE

15

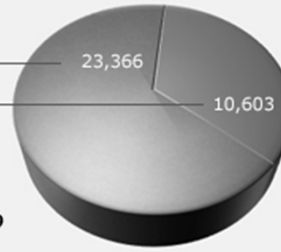


CLOSED INVESTIGATED CASES

Total Investigated Resolutions April 14, 2003 - January 31, 2015

Corrective Action Obtained
(Change Achieved) (69%)

No Violation (31%)



Total Complaints Investigated 33,969

HIPAA Summit

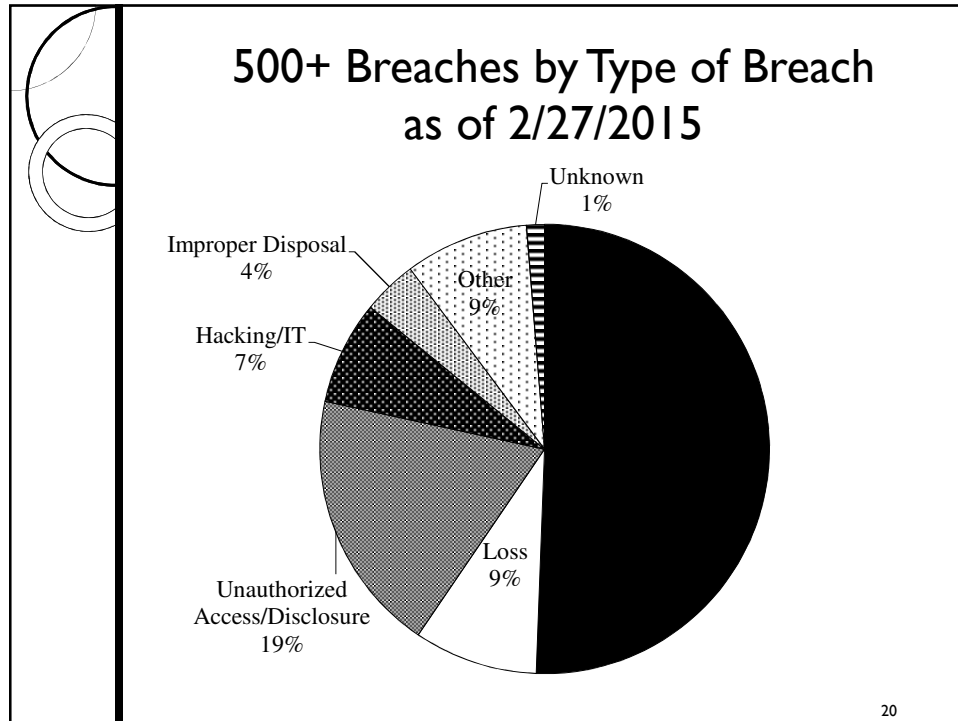
18

BREACH HIGHLIGHTS

September 2009 through February 27, 2015

- Approximately 1,144 reports involving a breach of PHI affecting 500 or more individuals
 - Theft and Loss are 60% of large breaches
 - Laptops and other portable storage devices account for 32% of large breaches
 - Paper records are 22% of large breaches
- Approximately 157,000+ reports of breaches of PHI affecting less than 500 individuals

19



Definition of Breach – New Rule

- Under the omnibus regulations, the “risk of harm” standard has been removed
- Impermissible use/disclosure of (unsecured) PHI is *presumed* to require the issuance of a breach notification, unless the CE/BA can demonstrate that there is a low probability that PHI has been compromised, based on a risk assessment of at least the following:
 - Nature and extent of the PHI involved
 - Who received/accessed the PHI
 - What is the potential that PHI was actually acquired or viewed
 - The extent to which risk to the data has been mitigated
- Exceptions for inadvertent, harmless mistakes remain
- Exception for limited data sets without dates of birth and zip codes has been removed

21

LESSONS LEARNED

Appropriate Safeguards Prevent Breaches

- Evaluate the risk to e-PHI when at rest on removable media, mobile devices and computer hard drives
- Take reasonable and appropriate measures to safeguard e-PHI
 - Store all e-PHI to a network
 - Encrypt data stored on portable/movable devices & media
 - Employ a remote device wipe to remove data when lost or stolen
 - Consider appropriate data backup
 - Train workforce members on how to effectively safeguard data and timely report security incidents

22

Eye to the Future

- Increased efficiency
- High-impact cases
 - Audit

HHS expects full compliance, no matter the size of a covered entity. Assure that policies relating to privacy, security and breach notification are up- to- date and effectively implemented.

23



HIPAA Privacy, Security, Breach Compliance and Enforcement – What’s to Come

Resolution Agreements/Corrective Action Plans

- Continue to increase activity and resources
- Maintain focus on fundamentals of compliance programs
- Address emerging issues


Investigated Complaints/Compliance Reviews

- New web portal for complaints/centralized intake
https://ocrportal.hhs.gov/ocr/cp/complaint_frontpage.jsf
- Strategic approach to increase efficiencies, identify cases for investigation

Breach Reports

- Redesigned website for 500+ postings
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>

24



NEW OCR RULES, GUIDANCE, AND TOOLS

25

CLIA Final Rule

- Joint Rulemaking
- Centers for Medicare and Medicaid Services (CMS) – Amended Clinical Laboratory Improvement Amendment Act of 1988 (CLIA) regulations to allow laboratories to give patients direct access to completed test results
- OCR – Amended HIPAA right to access to remove exemption for CLIA labs
 - Individual has right to get copy of test reports directly from labs
 - Access obligations on labs same as for other CEs
 - Individual can still go through physician to obtain test results
- Dates
 - Published February 6, 2014
 - Effective April 7, 2014
 - Compliance Required By October 6, 2014

Guidance Regarding HIPAA and Same-Sex Marriage

- In September 2014, OCR issued guidance for covered entities in implementing the United States Supreme Court's 2013 decision in *United States v. Windsor* in which the Court held Section 3 of the Defense of Marriage Act to be unconstitutional.
- The Guidance clarifies the definition of *family member* in the Privacy Rule. 45 CFR 160.103. Both *spouse* and *marriage* are included in that definition.



Informal Guidance on Privacy in Emergency Situations

- In November 2014, OCR issued informal guidance, in the form of a bulletin, regarding the ways in which covered entities and their business associates could share PHI in emergency situations, such as the Ebola outbreak, as well as the continuing duties to protect the privacy of patient information even in emergency situations.
- The bulletin largely focused on public health activities under the Privacy Rule.
- A link to the bulletin can be found on the OCR HIPAA home page. www.hhs.gov/ocr/hipaa.

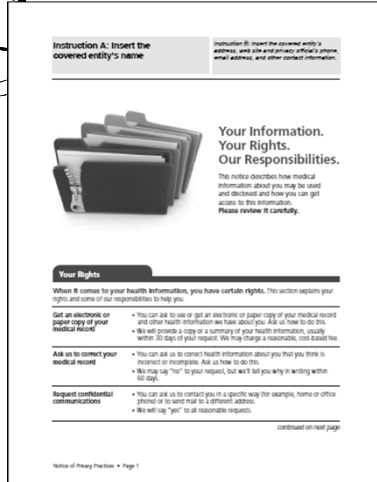
28



OCR RESOURCES

29

Model Notice of Privacy Practices



- Notice in the form of a booklet;
- A layered notice that presents a summary of the information on the first page, followed by the full content on the following pages;
- A notice with the design elements found in the booklet, but formatted for full page presentation.
- A text only version of the notice;
- Different versions for plans and health care providers.

<http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html>