# OCR 101 and Lessons Learned from HIPAA Breaches

**Presented to the Health Care Compliance Association- Seattle Regional Annual Conference**

**June 10, 2016**

**Sun Lee, J.D.**
**Equal Opportunity Specialist**
**U.S. Department of Health and Human Services**
**Office for Civil Rights**

## Agenda

- Overview of the Office for Civil Rights (OCR) and investigative processes
- Common breach issues
- General OCR audit updates
- Resources
- Questions

2

## Office for Civil Rights (OCR)

- Part of the U.S. Department of Health and Human Services (HHS)
- Enforces a number of civil rights laws as they relate to recipients of Federal financial assistance from HHS
- Enforces the HIPAA Privacy, Security, and Breach Notification Rules

3

## OCR REGIONAL OFFICES

OCR Regional Offices support headquarters through enforcement activities, conducting investigation and compliance reviews, public education, technical assistance and outreach.

- New England
- Eastern and Caribbean
- Mid-Atlantic
- Southeast
- Midwest
- Southwest
- Rocky Mountain
- Pacific


## Enforcement and Compliance Activities

- Complaint and breach investigations
- Compliance reviews
- Voluntary resolution agreements
- Formal enforcement
- Audits
- Outreach and public education
- Policy development

5

## Complaints

- Initiated by a member of the public
- Most resolved through other means rather than investigation
- Investigations are generally issue specific
- May include other issues as indicated by the investigation

6

## Complaints*

- 128,937 HIPAA complaints
- Common Complaints
  - Impermissible uses and disclosures of protected health information (PHI)
  - Lack of safeguards of PHI
  - Lack of patient access to their PHI
  - Lack of administrative safeguards of electronic protected health information (ePHI)
  - Use or disclosure of more than the minimum necessary PHI

*As of February 29, 2016

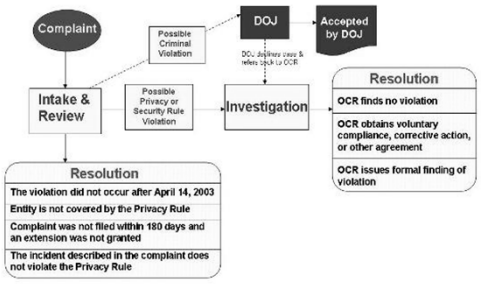
7

## Complaints- Technical Assistance

- Technical assistance and guidance on common privacy complaint issues available at:
  - http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/significant-aspects/index.html
- New guidance regarding individual access to protected health information:
  - http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/
- Technical assistance and guidance on the Security Rule, including basics of the Security Rule and Risk Analysis and Risk Management:
  - http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

8

## HIPAA Privacy & Security Rule Complaint Process




9

## Investigation Process

- Notice letter and Data Request
  - Due dates
  - Extensions
- Secondary data requests
- Witness interviews
- Site visit

10

## Resolution of Complaints

- Investigation outcomes
  - Voluntary corrective action
  - Unable to corroborate
  - No violation
- Closure letter

11

## Compliance Reviews

- Initiated by OCR
  - Complaint converted into a compliance review
  - Triggered by Breach Notification
  - Internal initiatives
- Numerous issues
- May include all three subparts (Privacy, Security, Breach Notification)

12

## Voluntary Corrective Action

- Entity will be asked to fix or change a finding from the investigation
- Change or correction will need to be documented
- May include a policy creation or amendment
- May include training or retraining

13

## Resolution Agreement and Corrective Action Plan

- Efforts at voluntary corrective action are unsuccessful
- Findings are egregious
- Still considered informal settlement
- Generally includes
  - Resolution amount
  - Corrective action plan
  - Monitoring period

14

## Formal Enforcement

- Informal settlement has failed - 30 days to raise any mitigating factors or affirmative defenses
- Notice of Proposed Determination lays out the proposed Civil Money Penalty - 90 days to request a hearing
  - Hearing is not requested, the penalty amount becomes final and enforceable
  - Hearing is requested, it is conducted before an administrative law judge

15

## Breach

"Breach:" Impermissible acquisition, access, use, or disclosure of PHI (paper or electronic), which compromises the security or privacy of the PHI

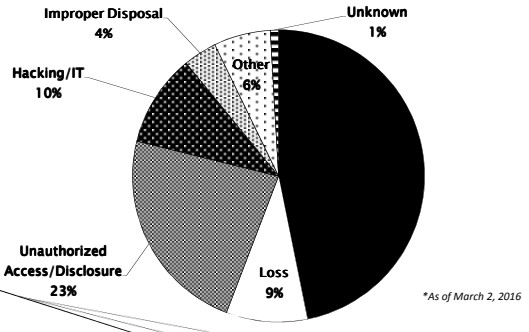
Breach is presumed, UNLESS:

- The CE or BA can demonstrate (through a documented risk assessment*) that there is a low probability that the PHI has been compromised based on:
  - Nature and extent of the PHI involved (including the types of identifiers and the likelihood of re-identification);
  - The unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether the PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been mitigated.

**See 45 C.F.R. Section 164.402 (2)*

16

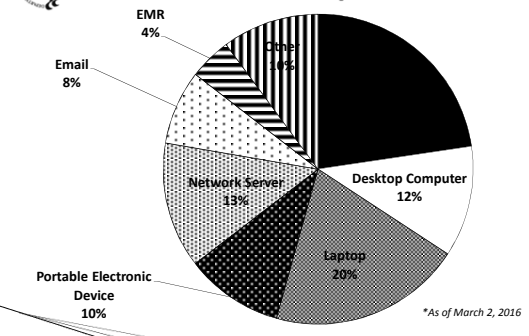
## Categories of Over 500 Breaches*




**As of March 2, 2016*

17

## 500+ Breaches by Location*




**As of March 2, 2016*

18

## Breaches

- September 2009 through March 2, 2016
  - Approximately 1,476 reports involving a breach of PHI affecting 500 or more individuals
  - Theft: 47% of 500+ breaches
  - Laptops and other portable storage devices: 30% of 500+ breaches
  - Paper records: 23% of 500+ breaches
- Approximately 222,430+ reports of breaches of PHI affecting fewer than 500 individuals

19

## Lack of Business Associate Agreements

- Covered entities and business associates must enter into agreements with their business associates to ensure that the business associates will appropriately safeguard PHI. *See* 45 C.F.R. § 164.308(b).
- Examples of potential Business Associates:
  - A collections agency providing debt collection services to a health care provider which involves access to PHI
  - An attorney whose legal services to a health plan involve access to PHI
  - An independent medical transcriptionist that provides transcription services to a physician
  - A subcontractor providing remote backup services of PHI data for an IT contractor-business associate of a health care provider

20

## Incomplete or Inaccurate Risk Analysis

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the [organization]. *See* 45 C.F.R. § 164.308(a)(1)(ii)(A).
- Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.

21

## Incomplete or Inaccurate Risk Analysis- cont'd

When identifying ePHI, be sure to consider:

- Applications (EHR, PM, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.)
- Computers (servers, workstations, laptops, virtual and cloud based systems, etc.)
- Medical Devices (tomography, radiology, DXA, EKG, ultrasounds, spirometry, etc.)
- Messaging Apps (email, texting, ftp, etc.)
- Mobile and Other Devices (tablets, smartphones, copiers, digital cameras, etc.)
- Media (tapes, CDs/DVDs, USB drives, memory cards, etc.)

22

## Failure to Manage Identified Risk, e.g. Encrypt

- The Risk Management Standard requires the "[implementation of] security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule]." *See* 45 C.F.R. § 164.308(a)(1)(ii)(B).
- Several instances of breaches where risks attributable to a reported breach had been previously identified as part of a risk analysis, but that the breaching organization failed to act on its risk analysis and implement appropriate security measures.
- In some instances, encryption was included as part of a remediation plan; however, activities to implement encryption were not carried out or were not implemented within a reasonable timeframe as established in a remediation plan.

23

## Risk Analysis and Risk Management Technical Assistance

- http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
  - Security Rule 101
  - Basics of Risk Analysis and Risk Management
  - National Institute of Standards and Technology (NIST) Special Publications
  - Information for small providers
- Security Risk Assessment Tool
  - https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

24

## Lack of Transmission Security

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate. *See* 45 C.F.R. § 164.312(e)(2)(ii).
- Applications for which encryption should be considered when transmitting ePHI may include:
  - Email
  - Texting
  - Application sessions
  - File transmissions (e.g., ftp)
  - Remote backups
  - Remote access and support sessions (e.g., VPN)

25

## Lack of Appropriate Auditing

- The HIPAA Rules require the "[implementation] of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." *See* 45 C.F.R. § 164.312(b).
- Once audit mechanisms are put into place on appropriate information systems, procedures must be implemented to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." *See* 45 C.F.R. § 164.308(a)(1)(ii)(D).

26

## Lack of Appropriate Auditing-cont'd

- Activities which could warrant additional investigation:
  - Access to PHI during non-business hours or during time off
  - Access to an abnormally high number of records containing PHI
  - Access to PHI of persons for which media interest exists
  - Access to PHI of employees

27

## No Patching of Software

- The use of unpatched or unsupported software on systems which access ePHI could introduce additional risk into an environment.
- Continued use of such systems must be included within an organization's risk analysis and appropriate mitigation strategies implemented to reduce risk to a reasonable and appropriate level.

28

## No Patching of Software-cont'd

- In addition to operating systems, EMR/PM systems, and office productivity software, software which should be monitored for patches and vendor end-of-life for support include:
  - Router and firewall firmware
  - Anti-virus and anti-malware software
  - Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

29

## Improper Disposal

- When an organization disposes of electronic media which may contain ePHI, it must implement policies and procedures to ensure that proper and secure disposal processes are used. *See* 45 C.F.R. § 164.310(d)(2)(i).
- The implemented disposal procedures must ensure that "[e]lectronic media have been cleared, purged, or destroyed consistent with *NIST Special Publication 800–88: Guidelines for Media Sanitization*, such that the PHI cannot be retrieved."

30

## Improper Disposal- cont'd

- Electronic media and devices identified for disposal should be disposed of in a timely manner to avoid accidental improper disposal.
- Organizations must ensure that all electronic devices and media containing PHI are disposed of securely; including non-computer devices such as copier systems and medical devices.

31

## Recent Enforcement Actions

- **Complete PT (February 2016)**
  - Posting of PHI on web site without patient authorization
  - Failure to safeguard; no policies and procedures for obtaining authorization
  - Corrective action plan and $25,000 settlement amount
- **Lincare (February 2016)**
  - PHI of 278 patients removed from company office, left exposed and then abandoned altogether
  - Inadequate policies and procedures to safeguard PHI taken offsite even though frequent practice; unwritten policy for storing PHI in vehicles
  - $239,800 civil money penalty

32

## Recent Enforcement Actions

- **Triple-S Management Corp (November 2015)**
  - Multiple breaches
  - Failure to safeguard, impermissible disclosure of PHI to vendor without business associate agreement, failure to use or disclose "minimum necessary" PHI, failure to conduct accurate and thorough risk analysis and conduct appropriate security management
  - Corrective action plan and $3.5 million settlement amount
- **Lahey Hospital and Medical Center (November 2015)**
  - Theft of laptop containing PHI of 599 individuals from a stand that accompanied portable CT scanner
  - Failure to conduct thorough risk analysis, lack of appropriate policies and procedures to safeguard PHI maintained on workstations used with diagnostic/lab equipment, lack of unique credentials, failure to examine system activity
  - Corrective action plan and $850,000 settlement amount

33

## OCR Audit Updates

- Background
- Updates
- More information:
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

34

## Resources

- The OCR website, http://www.hhs.gov/hipaa/index.html offers a wide range of helpful information about health information privacy including educational information, FAQ's, rule text and guidance for the Privacy, Security, and Breach Notification Rules.
- OCR sample forms include:
  - Model Notice of Privacy Practices:
    - http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/
  - Sample Business Associate Agreement:
    - http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

35

## Resources

- Enforcement highlights: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html
- More information and case examples at OCR's web site: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/index.html
- The HealthIT.gov website has excellent information and videos on securing mobile devices and on how to implement HIPAA Privacy and Security Rules: http://www.healthit.gov/providers-professionals/ehr-privacy-security

36

## Questions

- www.hhs.gov/ocr
- Contact information:
  Sun.Lee@hhs.gov
  206-615-3873 (Office)

37