What's New with HIPAA? Enforcement Update

HHS Office for Civil Rights

Precision Medicine and Access Guidance

- OCR provided guidance on individuals' access to their protected health information under the Privacy Rule in two releases. The second release included detailed guidance on permissible fees.
- http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Ransomware Guidance

- OCR recently released guidance on ransomware. The new guidance reinforces activities required by HIPAA that can help organizations prevent, detect, contain, and respond to threats.
- http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Cloud Computing Guidance

- OCR released guidance clarifying that a CSP is a business associate – and therefore required to comply with applicable HIPAA regulations – when the CSP creates, receives, maintains or transmits identifiable health information (referred to in HIPAA as electronic protected health information or ePHI) on behalf of a covered entity or business associate.

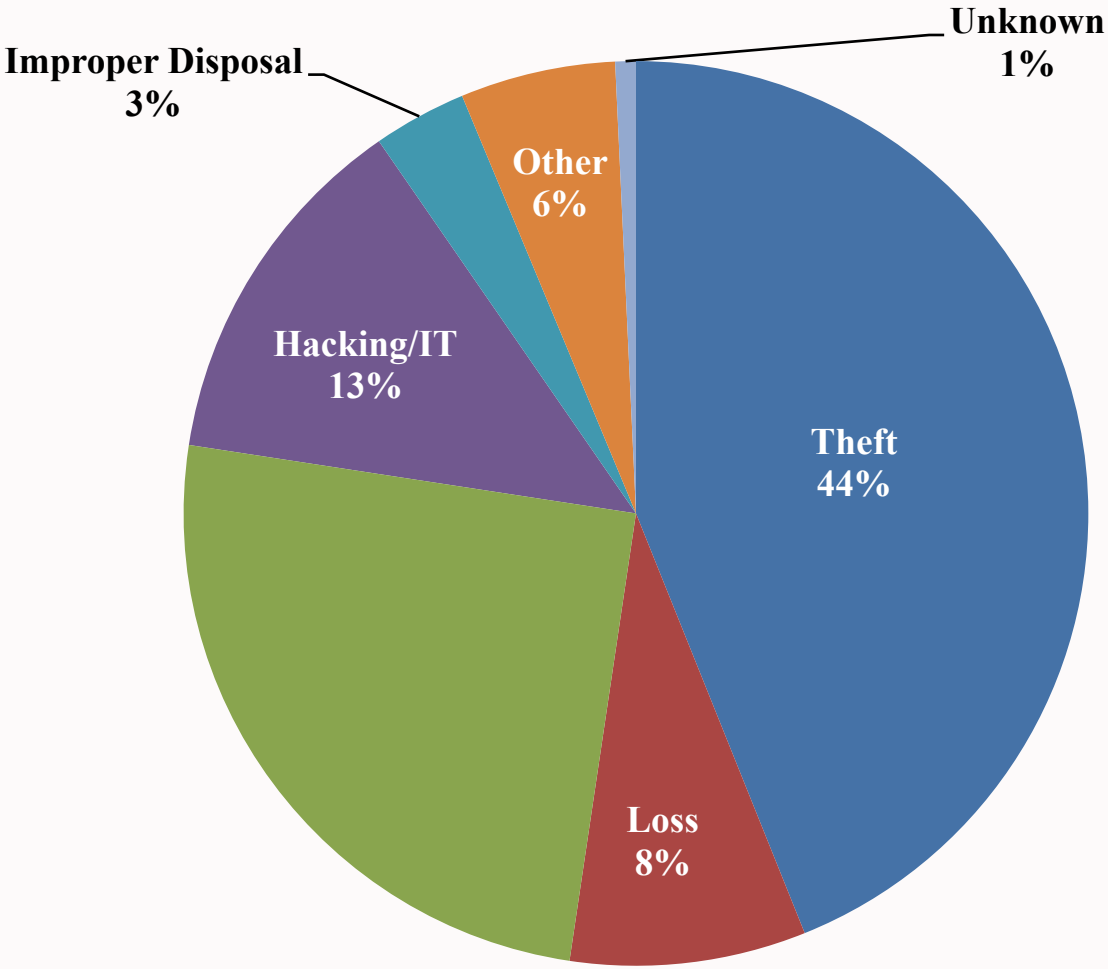
- When a CSP stores and/or processes ePHI for a covered entity or business associate, that CSP is a business associate under HIPAA, even if the CSP stores the ePHI in encrypted form and does not have the key.

- CSPs are not likely to be considered "conduits," because their services typically involve storage of ePHI on more than a temporary basis.
- http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- http://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html

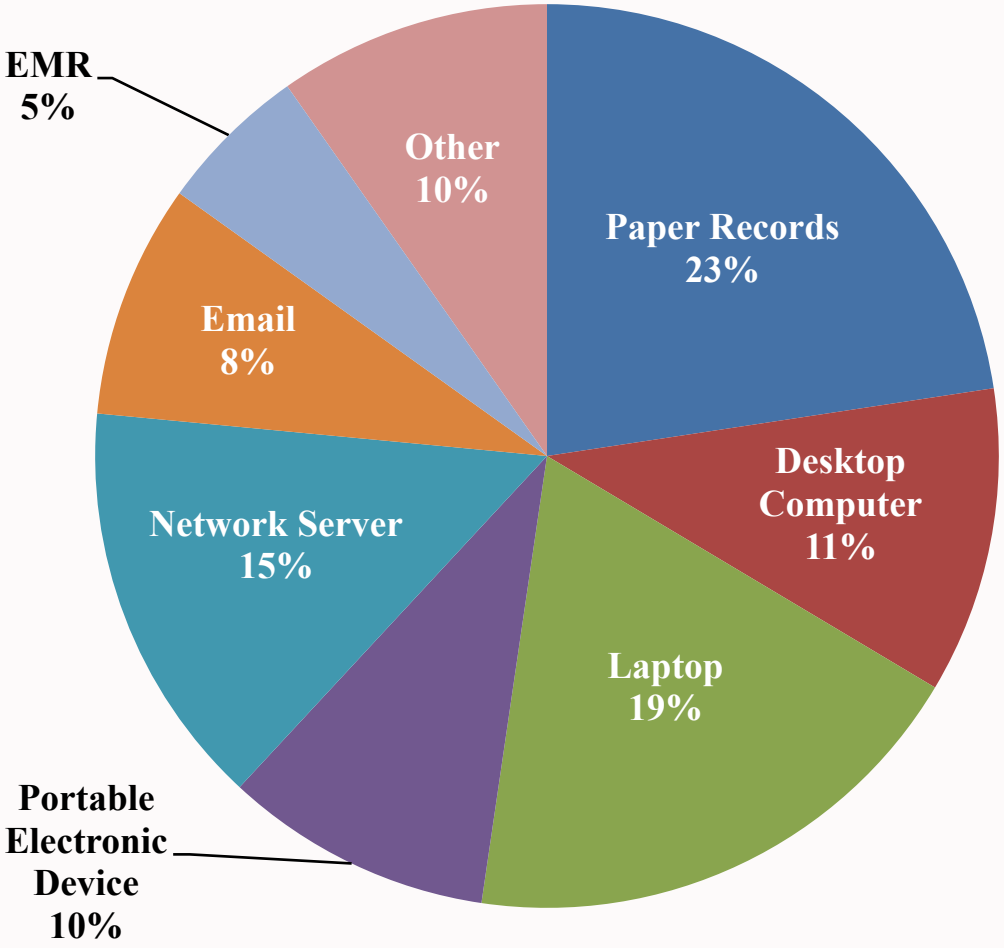
September 2009 through September 30, 2016

- Approximately 1,688 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 52% of large breaches
  - Hacking/IT now account for 13% of incidents
  - Laptops and other portable storage devices account for 29% of large breaches
  - Paper records are 23% of large breaches
  - Individuals affected are approximately 168,814,997
- Approximately 239,362 reports of breaches of PHI affecting fewer than 500 individuals

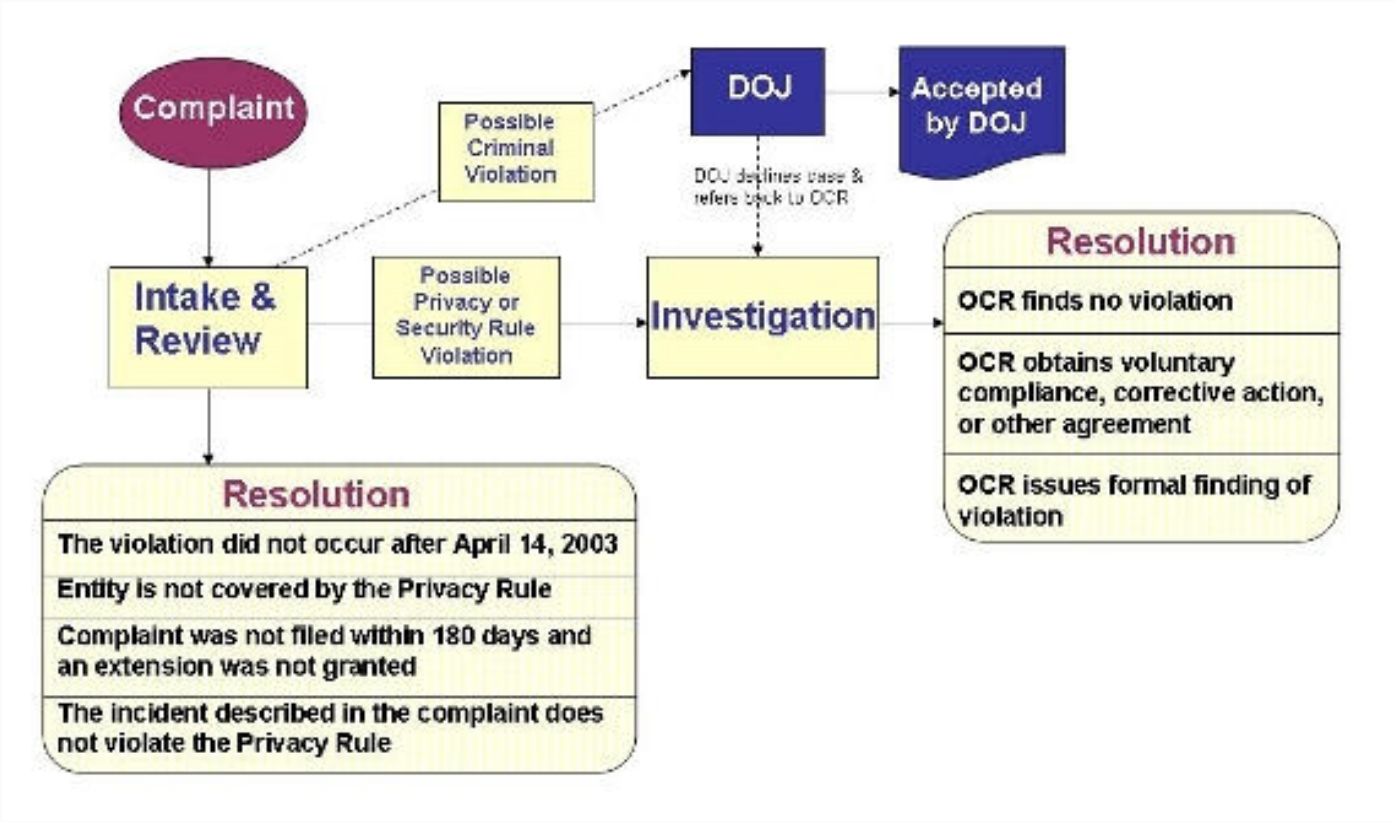
500+ Breaches by Type of Breach as of September 30, 2016



500+ Breaches by Location of Breach as of September 30, 2016



HIPAA Privacy and Security Rule Complaint Process



Lack of Business Associate Agreements

- The HIPAA Rules generally require that covered entities and business associates enter into agreements with their business associates to ensure that the business associates will appropriately safeguard protected health information. 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 protected health information.
  - An attorney whose legal services to a health plan involve access to protected health information.
  - 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.

Incomplete or Inaccurate Risk Analysis

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information 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.
- 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.)

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- http://scap.nist.gov/hipaa/
- http://www.healthit.gov/providers-professionals/security-risk-assessment

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).
- Investigations conducted by OCR regarding several instances of breaches uncovered that 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.

http://www.healthit.gov/mobiledevices

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)

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).
- 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

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.
- 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.)

Insider Threat

- Organizations must "[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information … and to prevent those workforce members who do not have access … from obtaining access to electronic protected health information," as part of its Workforce Security plan. See 45 C.F.R. § 164.308(a)(3).
- Appropriate workforce screening procedures could be included as part of an organization's Workforce Clearance process (e.g., background and OIG LEIE checks). See 45 C.F.R. § 164.308(a)(3)(ii)(B).
- Termination Procedures should be in place to ensure that access to PHI is revoked as part of an organization's workforce exit or separation process. See 45 C.F.R. § 164.308(a)(3)(ii)(C).

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."
- 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.

Insufficient Data Backup and Contingency Planning

- Organizations must ensure that adequate contingency plans (including data backup and disaster recovery plans) are in place and would be effective when implemented in the event of an actual disaster or emergency situation. See 45 C.F.R. § 164.308(a)(7).
- Leveraging the resources of cloud vendors may aid an organization with its contingency planning regarding certain applications or computer systems, but may not encompass all that is required for an effective contingency plan.
- As reasonable and appropriate, organizations must periodically test their contingency plans and revise such plans as necessary when the results of the contingency exercise identify deficiencies. See 45 C.F.R. § 164.308(a)(7)(ii)(D).

- HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements – September 23, 2016
- Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million - August 4, 2016
- Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC) - July 21, 2016
- Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University - July 18, 2016
- Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement – June 29, 2016
- Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital - April 21, 2016
- $750,000 settlement highlights the need for HIPAA business associate agreements
- Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement - March 17, 2016
- $1.55 million settlement underscores the importance of executing HIPAA business associate agreements - March 16, 2016
- Physical therapy provider settles violations that it impermissibly disclosed patient information - February 16, 2016
- Administrative Law Judge rules in favor of OCR enforcement, requiring Lincare, Inc. to pay $239,800 - February 3, 2016

http://www.hhs.gov/hipaa/for-professionals/security/index.html

- The Security Rule
- Security Rule History
- Security Rule Guidance and Notices
- NIST Toolkit
- FAQs

QUESTIONS?