NIST and OCR Conference 2017

Important Guidance: Emergency Preparedness and Emergency Situations

- Hurricane Harvey:
  - https://www.hhs.gov/sites/default/files/hurricane-harvey-hipaa-bulletin.pdf
- Family and Friends:
  - https://www.hhs.gov/sites/default/files/provider_ffg.pdf

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Cyber Security Guidance Webpage

- Cyber Security Guidance Material Webpage

  https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

- Includes a Cyber Security Checklist and Infographic, which explain the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.
  - Cyber Security Checklist - PDF
  - Cyber Security Infographic [GIF 802 KB]

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Additional Cybersecurity Guidance: Ransomware and Cloud Computing

- Ransomware:
  - http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- NIST Cybersecurity Crosswalk with HIPAA Mapping:
  - https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf?language=es

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Monthly Guidance: Cybersecurity Newsletters

February 2016	Ransomware, “Tech Support” Scam, New BBB Scam Tracker
March 2016	Keeping PHI safe, Malware and Medical Devices
April 2016	New Cyber Threats and Attacks on the Healthcare Sector
May 2016	Is Your Business Associate Prepared for a Security Incident
June 2016	What’s in Your Third-Party Application Software
September 2016	Cyber Threat Information Sharing
October 2016	Mining More than Gold (FTP)
November 2016	What Type of Authentication is Right for you?
December 2016	Understanding DoS and DDoS Attacks
January 2017	Audit Controls
February 2017	Reporting and Monitoring Cyber Threats
March 2017	Reporting and Monitoring Cyber Threats
April 2017	Man-in-the-Middle Attacks and “HTTPS Inspection Products”
May 2017	Cybersecurity Incidents will happen…Remember to Plan, Respond, and Report!
June 2017	File Sharing and Cloud Computing: What to Consider?
July 2017	Train Your Workforce, so They Don’t Get Caught by a Phish!
August 2017	Protecting yourself from potential scammers while being charitable

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

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

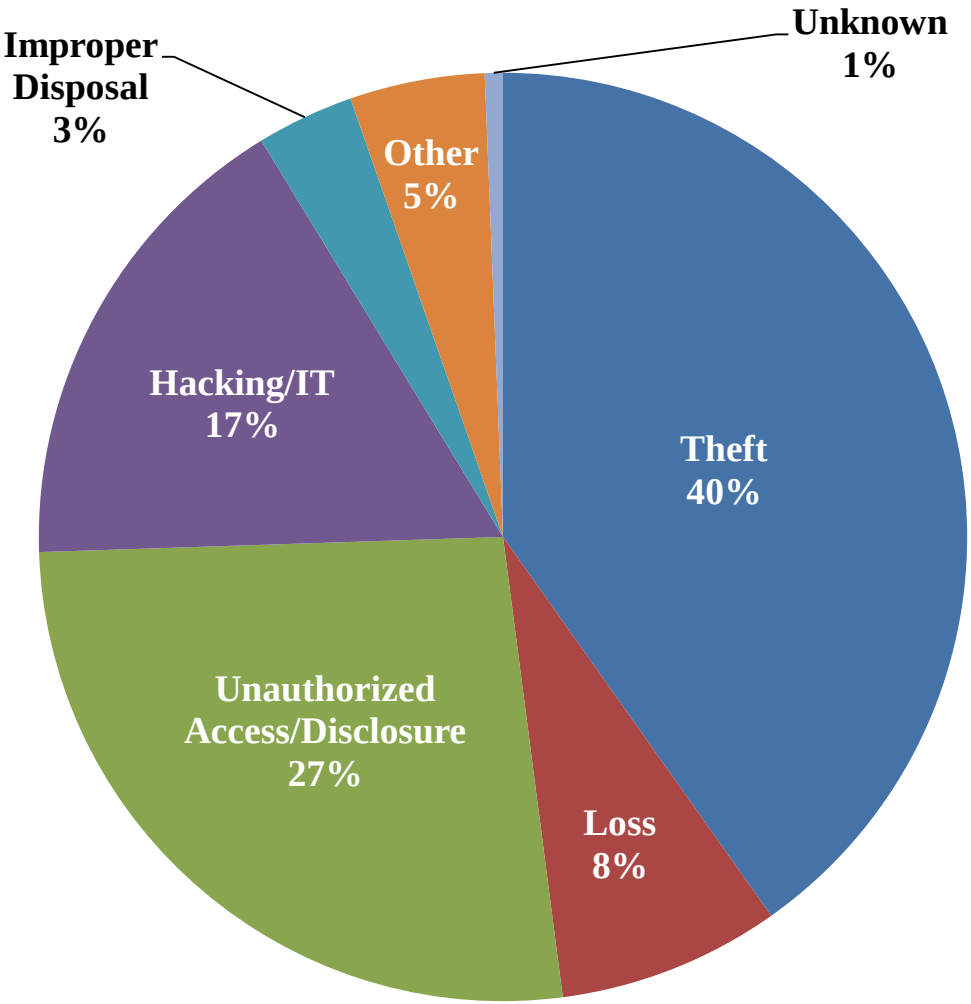
HIPAA Breach Highlights

September 2009 through July 31, 2017

- Approximately 2,017 reports involving a breach of PHI affecting 500 or more individuals
- Theft and Loss are 48% of large breaches
- Hacking/IT now account for 17% of incidents
- Laptops and other portable storage devices account for 26% of large breaches
- Paper records are 21% of large breaches
- Individuals affected are approximately 174,974,489
- Approximately 293,288 reports of breaches of PHI affecting fewer than 500 individuals

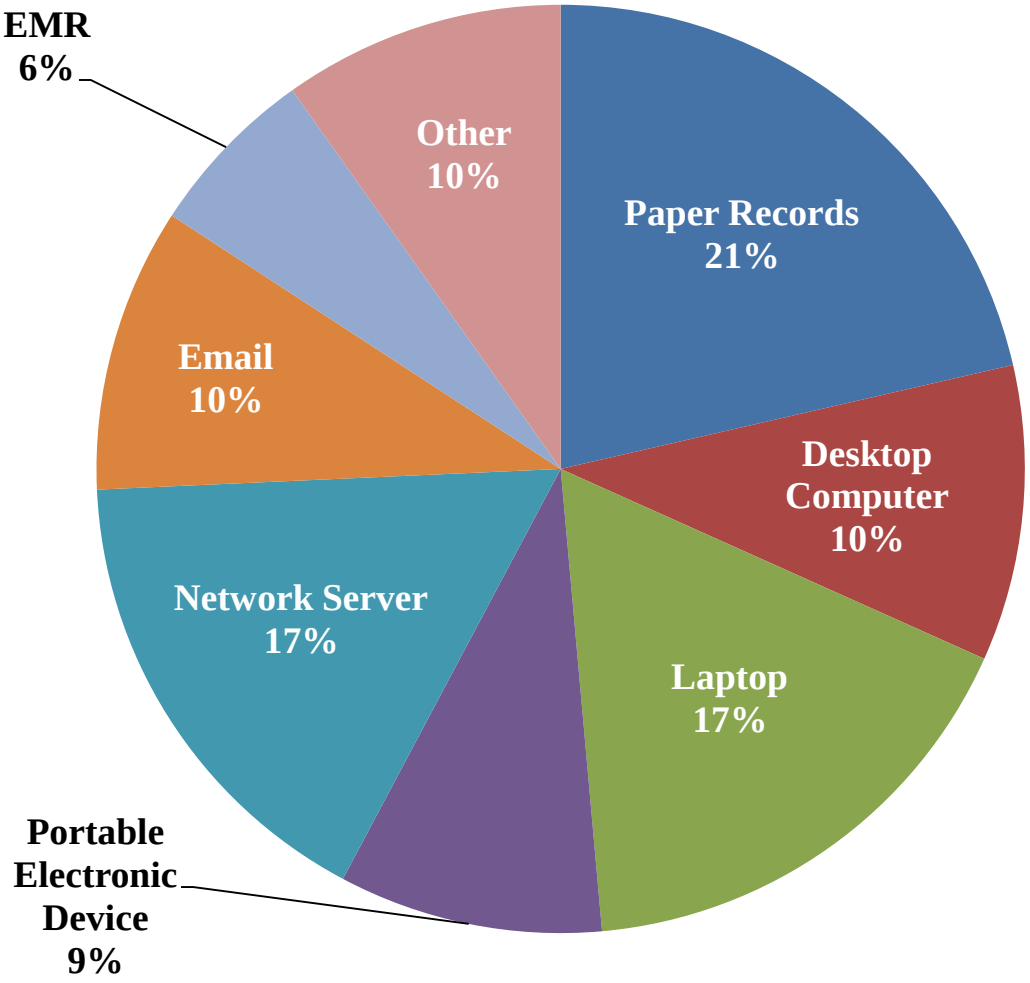
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

500+ Breaches by Type of Breach as of July 31, 2017



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

500+ Breaches by Location of Breach as of July 31, 2017



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Complaints Received and Cases Resolved

- Over 158,293 complaints received to date
- Over 25,312 cases resolved with corrective action and/or technical assistance
- Expect to receive 17,000 complaints this year

Enforcement Guidance: How OCR Closes Cases

- https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html
- Cases that OCR closes fall into five categories:
  - Resolved after intake & review (no investigation)
  - Technical Assistance (no investigation)
  - No Violation (investigated)
  - Corrective Action Obtained (investigated; includes Resolution Agreements)
- OCR may decide not to investigate a case further if :
  - The case is referred to the Department of Justice for prosecution.
  - The case involved a natural disaster.
  - The case was pursued, prosecuted, and resolved by state authorities.
  - The covered entity or business associate has taken steps to comply with the HIPAA Rules and OCR determines enforcement resources are better/more effectively deployed in other cases.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Recent Enforcement Actions

- https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
- 5/23/2017: Careless handling of HIV information jeopardizes patient's privacy
- 5/10/2017: Texas health system settles potential HIPAA violations for disclosing patient information
- 4/24/2017: Settlement shows that not understanding HIPAA requirements creates risk
- 4/20/2017: No Business Associate Agreement?
- 4/12/2017: Overlooking risks leads to breach
- 2/16/2017: HIPAA settlement shines light on the importance of audit controls
- 2/1/2017: Lack of timely action risks security and costs money
- 1/18/2017: HIPAA settlement demonstrates importance of implementing safeguards for ePHI

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Continuing Enforcement Issue: Affirmative Disclosures Not Permitted

The HIPAA Privacy Rule provides that Covered Entities or Business Associates may not use or disclose PHI except as permitted or required. See 45 C.F.R. § 164.502(a). Examples of Potential Violations:

- Covered Entity permits news media to film individuals in its facility prior to obtaining their authorization.
- Covered Entity publishes PHI on its website or on social media without an authorization from the individual(s).
- Covered Entity confirms that an individual is a patient and provides other PHI to reporter(s) without authorization from the individual.
- Covered Entity faxes PHI to an individual's employer without authorization from the individual.

Continuing Enforcement Issue: Lack of Business Associate Agreements

HIPAA generally requires 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 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.

Continuing Enforcement Issue: 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.
- Examples: Applications like EHR, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.); Cloud based servers; Medical Devices Messaging Apps (email, texting, ftp); Media

Risk Analysis Guidance

- 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

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Continuing Enforcement Issue: Failure to Manage Identified Risk

- 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.

Mobile Device Security

http://www.healthit.gov/mobiledevices

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

Continuing Enforcement Issue: 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)

Continuing Enforcement Issue: 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

Continuing Enforcement Issue: 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.)

Continuing Enforcement Issue: 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).

Continuing Enforcement Issue: Disposal of PHI

- 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.

Continuing Enforcement Issue: Insufficient 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 164.308(a)(7)(ii)(D).

Questions

- http://www.hhs.gov/hipaa
- Join us on Twitter @hhsocr

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS