United States Department of Health & Human Services
Office for Civil Rights

# What's New with HIPAA? Policy and Enforcement Update

HHS Office for Civil Rights

United States Department of Health & Human Services
Office for Civil Rights

**New Initiatives**

- Precision Medicine Initiative (PMI), including Access Guidance
- Cybersecurity
- Developer portal
- NICS Final Rule



United States Department of Health & Human Services
Office for Civil Rights



**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

United States Department of Health & Human Services
Office for Civil Rights
Cybersecurity

**NIST Cybersecurity Framework**

- OCR released a crosswalk, developed with NIST and ONC, that identifies "mappings" between the NIST Framework for Improving Critical Infrastructure Cybersecurity (the Cybersecurity Framework) and the Security Rule. The crosswalk also includes mappings to other commonly used security frameworks.
- http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html

4

United States Department of Health & Human Services
Office for Civil Rights
NICS Final Rule

**NICS Final Rule**

- OCR modified the Privacy Rule Privacy Rule to expressly permit certain covered entities to disclose to the National Instant Criminal Background Check System (NICS) the identities of those individuals who, for specific mental health reasons, already are prohibited by Federal law from having a firearm.
- http://www.hhs.gov/blog/2016/01/04/obama-administration-modifies-hipaa.html

5

United States Department of Health & Human Services
Office for Civil Rights
mHealth Portal

**HIT Developer Portal**

- OCR has launched a platform for mobile health developers; purpose is to understand concerns of developers new to health care industry and HIPAA standards
  - Users can submit questions, comment on other submissions, vote on relevancy of topic.
  - Will consider comments as we develop our priorities for additional guidance and technical assistance
- http://hipaaQsportal.hhs.gov/

6

United States Department of Health & Human Services
Office for Civil Rights

*Developing Policy*

## In Development

- Cloud Computing Guidance
- ANPRM to solicit views on ways in which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any CMP or monetary settlement collected



United States Department of Health & Human Services
Office for Civil Rights

*Audit Program*

- OCR is using FCi Federal contractors to help support the next phase of the audit program. They have been trained and are working closely with OCR in-house.
- OCR has been verifying contact information for business associates and covered entities to be included in the next round of audit activities
- Next round will mostly consist of desk audits, although some on-site audits should also be expected
- Additional information on OCR's website.



United States Department of Health & Human Services
Office for Civil Rights

*Breach Notification Rule*

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

Safe Harbor: If the PHI is encrypted or destroyed.

Breach is Presumed and Must Be Reported, 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.

Focus on risk to the data, instead of risk of harm to the individual.

United States Department of Health & Human Services
Office for Civil Rights

## Breach Risk Assessment

Covered entity/business associate has burden of proof to demonstrate all notifications were made or notifications not required:

- Document that notifications made in timely manner; or
- Document risk assessment demonstrating low probability of compromise of data or that exception applies.

Risk assessment must be thorough (addressing at minimum all four required factors), completed in good faith, and reasonable.



United States Department of Health & Human Services
Office for Civil Rights

## Breach Reporting Highlights

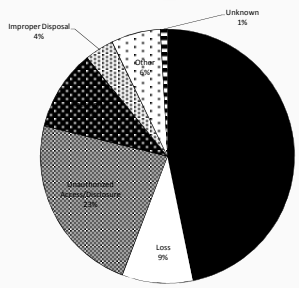
September 2009 through March 2, 2016

- Approximately 1,476 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 47% of large breaches
  - Laptops and other portable storage devices account for 20% of large breaches
  - Paper records are 23% of large breaches
- Approximately 222,430+ reports of breaches of PHI affecting fewer than 500 individuals



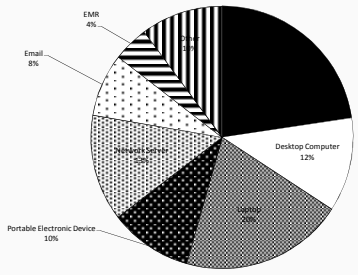
United States Department of Health & Human Services
Office for Civil Rights

## 500+ Breaches by Type of Breach



United States Department of Health & Human Services
Office for Civil Rights

500+ Breaches by Location




OCR Activity Update 13

United States Department of Health & Human Services
Office for Civil Rights

# Security Rule

OCR Activity Update 14

United States Department of Health & Human Services
Office for Civil Rights

Business Associate Agreements

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.

OCR Activity Update 15

United States Department of Health & Human Services
Office for Civil Rights

Risk Analysis

## 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.)

OCR Activity Update 16

United States Department of Health & Human Services
Office for Civil Rights

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


OCR Activity Update 17

United States Department of Health & Human Services
Office for Civil Rights

Risk Management

## 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.

OCR Activity Update 18

United States Department of Health & Human Services
Office for Civil Rights

*Mobile Device Security*

http://www.healthit.gov/mobiledevices




United States Department of Health & Human Services
Office for Civil Rights

*Transmission Security*

## 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)



United States Department of Health & Human Services
Office for Civil Rights

*Auditing*

## 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

United States Department of Health & Human Services
Office for Civil Rights



## 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.)



United States Department of Health & Human Services
Office for Civil Rights



## 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).



United States Department of Health & Human Services
Office for Civil Rights



## 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).





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

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



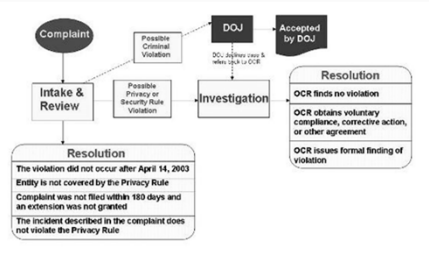


## Enforcement

United States Department of Health & Human Services
Office for Civil Rights

ENFORCEMENT PROCESS

## HIPAA Privacy and Security Rule Complaint Process






United States Department of Health & Human Services
Office for Civil Rights

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



United States Department of Health & Human Services
Office for Civil Rights

Recent Enforcement Actions

- U of Washington Medicine (December 2015)
  - Malware compromised IT system and PHI of approximately 90,000 individuals
  - Did not ensure affiliated entities were properly conducting risk analyses and appropriately responding to potential risk and vulnerabilities
  - Corrective action plan and $750,000 settlement amount
- 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

United States Department of Health & Human Services
Office for Civil Rights

Recent Enforcement Actions

- Lahey Hospital and Medical Center (November 2015)
  - Theft of laptop containing PHI of 599 individuals from 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



United States Department of Health & Human Services
Office for Civil Rights

Recent Enforcement Actions

- Cancer Care Group (September 2015)
  - Unencrypted computer and backup media stolen from employee's car, containing the PHI of approximately 55,000 current and former patients
  - No enterprise-wide risk analysis in place at time of breach; no written policy specific to the removal of hardware and electronic media containing ePHI into and out of facilities, even though common practice
  - Corrective action plan and $750,000 settlement amount
- St. Elizabeth's Medical Center (July 2015)
  - Internet-based document sharing application used to store PHI of patients; entity failed to analyze risks and failed to timely identify and respond to the incident
  - Also separate breach involving laptop and USB drive
  - Corrective action plan and $218,400 settlement amount



United States Department of Health & Human Services
Office for Civil Rights

QUESTIONS?