Updates

- Policy Development
- Breach Notification
- Enforcement
- HITECH Audit
HIPAA Right of Access Guidance

- Issued in two phases in early 2016
- Comprehensive Fact Sheet
- Series of FAQs
- Scope
- Form and Format and Manner of Access
- Timeliness
- Fees
- Directing Copy to a Third Party, and Certain Other Topics

HIT Developer Portal

- OCR launched platform for mobile health developers in October 2015; 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
- OCR will consider comments as we develop our priorities for additional guidance and technical assistance
- Guidance issued in February 2016 about how HIPAA might apply to a range of health app use scenarios
- FTC/ONC/OCR/FDA Mobile Health Apps Interactive Tool on Which Laws Apply issued in April 2016

Platform for users to influence guidance
http://hipaaQsportal.hhs.gov/
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

Cybersecurity Guidance Material

- HHS OCR has launched a Cyber Security Guidance Material webpage, including 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]
  

Cybersecurity Newsletters

- 15 issues in total
- 2017 Newsletters
  - May 2017 (Plan, Respond, and Report!)
  - June 2017 (File Sharing and Cloud Computing)
  - July 2017 (Workforce Training and Phishing)
  - August 2017 (Protecting Yourself from Scammers)

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.

Breach Highlights and Recent Enforcement Activity

- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach.
- Business associate must notify covered entity of breach.
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach.
- Annual reporting to HHS of smaller breaches (affecting less than 500 individuals) permitted.
- OCR posts breaches affecting 500+ individuals on OCR website.

Breach Notification Requirements
September 2009 through August 2017
- Approximately 2,049 reports involving a breach of PHI affecting 500 or more individuals
- Theft and Loss are 48% of large breaches
- Hacking/IT now account for 18% 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 175,674,825
- Approximately 295,811 reports of breaches of PHI affecting fewer than 500 individuals

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

HIPAA Breach Highlights
500+ Breaches by Type of Breach as of August 31, 2017

- Unauthorized Access/Disclosure: 26%
- Loss: 9%
- Theft: 40%
- Improper Disposal: 3%
- Other: 5%
- Unknown: 1%

HIPAA Breach Highlights
500+ Breaches by Location of Breach as of August 31, 2017

- Paper Records: 21%
- Desktop Computer: 10%
- Laptop: 17%
- Portable Electronic Device: 9%
- Network Server: 17%
- Email: 10%
- EMR: 6%
- Other: 10%
What Happens When HHS/OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
- OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
  - Entity's compliance prior to breach

Public can search and sort posted breaches

OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches

Investigations involve looking at:

- Underlying cause of the breach
- Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
- Entity's compliance prior to breach

Complaints Received and Cases Resolved

- Over 159,633 complaints received to date
- Over 25,373 cases resolved with corrective action and/or technical assistance
  - Expect to receive 17,000 complaints this year

How OCR Closes Cases

- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 49 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 civil money penalties
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html
Recent OCR enforcement
- Lessons learned

2017 Enforcement Actions
- Presence Health (Jan)
- MAPFRE Life Insurance Company of Puerto Rico (Jan)
- Children’s Medical Center of Dallas (Feb)
- Memorial Healthcare System (Feb)
- Metro Community Provider Network (April)
- Center for Children’s Digestive Health (April)
- CardioNet (April)
- Memorial Hermann Health System (May)
- St. Luke’s-Roosevelt Hospital Center, Inc. (May)

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 who 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)(i)(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://scap.nist.gov/

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.
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)

**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES**

**OFFICE FOR CIVIL RIGHTS**

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(b)(1)(i)(B).
- 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

**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES**

**OFFICE FOR CIVIL RIGHTS**

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.)

**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES**

**OFFICE FOR CIVIL RIGHTS**
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).

OFFICE FOR CIVIL RIGHTS

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 “electronic 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.

OFFICE FOR CIVIL RIGHTS

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).

OFFICE FOR CIVIL RIGHTS
Corrective Actions May Include:
- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- Implementing specific technical or other safeguards
- Mitigation
- CAPs may include monitoring

Some Good Practices
- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members’ critical role in protecting privacy and security

HITECH Audit
Audit Purpose:
Support Improved Compliance
- Identify best practices; uncover risks & vulnerabilities; detect areas for technical assistance; encourage consistent attention to compliance
- Intended to be non-punitive, but OCR can open up compliance review (for example, if significant concerns are raised during an audit or an entity fails to respond)
- Also hope to learn from this next phase in structuring permanent audit program

Audit Program Status
- Desk audits underway
- 167 Covered Entities
- 43 Business Associates
- Business Associate selection pool largely drawn from over 20,000 entities identified by audited CEs
- On-site audits of both CEs and BAs in 2017, after completion of the desk audit process, to evaluate against a comprehensive selection of controls in protocols
- A desk audit subject may be subject to on-site audit
- OCR beginning distribution of draft findings

Desk Audit Reporting: Process
After review of submitted documentation:
- Draft findings shared with the entity
- Entity may respond in writing
Final audit reports will:
- Describe how the audit was conducted
- Present any findings, and
- Contain any written entity responses to the draft
Covered Entity Desk Audit Controls

Privacy Rule Controls
- Notice of Privacy Practices & Content Requirements
  [§164.520(a)(1) & (b)(1)]
- Protection of Notice - Electronic Notice
  [§164.520(a)(3)]
- Right to Access
  [§164.524(a)1, (a)2, (a)3, (a)4, (a)5, (a)6, (a)7, (a)8, (a)9]

Breach Notification Rule Controls
- Timeliness of Notification
  [§164.406(b)]
- Content of Notification
  [§164.406(a)]

Security Rule Controls
- Security Management Process – Risk Analysis
  [§164.308(a)(1)(ii)(A)]
  [§164.308(a)(1)(ii)(B)]

Business Associate Desk Audit Controls

Breach Notification Rule Controls
- Notification by a Business Associate
  [§164.410, with reference to Content of Notification
  §164.406(a)]

Security Rule Controls
- Security Management Process – Risk Analysis
  [§164.308(a)(1)(ii)(A)]
  [§164.308(a)(1)(ii)(B)]

Audit Guidance

Selected protocol elements with associated document submission requests and related Q&As

Slides from audited entity webinar held July 13, 2016

Comprehensive question and answer listing

OCR Website:
http://www.hhs.gov/ocr/privacy/hipaa/compliance-enforcement/audit/index.html
Questions

- [http://www.hhs.gov/hipaa](http://www.hhs.gov/hipaa)
- Join us on Twitter @hhsoocr
- OCR Privacy and Security Listserv
  - [https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html](https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html)