HIPAA Privacy, Security – Lessons from 2016 and What's Next in 2017
Session 9, February 20, 2017
Deven McGraw, Deputy Director, Health Information Privacy
HHS Office for Civil Rights
Speaker Introduction

Deven McGraw, JD, MPH
Deputy Director
Health Information Privacy Division
HHS Office for Civil Rights
Conflict of Interest

Deven McGraw, JD, MPH

Has no real or apparent conflicts of interest to report.
Agenda

- 2017 Goals and Objectives
- Phase 2 Audits
- Compliance and Enforcement
- Cybersecurity Efforts
Learning Objectives

• Recognize OCR’s 2017 Goals and Objectives
• Discuss OCR’s Phase 2 Audit Program
• Compare OCR’s 2016 and 2017 Compliance and Enforcement Actions
• Illustrate OCR’s Cybersecurity Efforts
Electronic Secure Data, Enhanced Communication
2017 – Goals and Objectives

• Administration transition - new priorities could be set

• Staff have developed recommendations for additional policy guidance (plus additional responsibilities re: implementation of the 21st Century Cures Act).

• Continued execution of audit and enforcement of compliance with HIPAA Rules.
21st Century Cures Act

Calls for additional guidance:

• Accessing and sharing PHI for research purposes, including prep to research

• w/ONC, common legal, governance and security barriers that prevent trusted exchange of health info

• w/ONC, improving individual access to health information, including from BAs

• Ability to disclose treatment-related information about persons with mental health disorders, such as with close friends and family
Long-term Regulatory Agenda

• HITECH provision re: providing individuals harmed by violations of the HIPAA regulations with a percentage of any civil monetary penalties or settlements collected.

• HITECH provisions re: changes to HIPAA Accounting of Disclosure provisions.
Other guidance/FAQs

• Privacy and Security for “All of Us” (PMI) research program
• Text messaging
• Social Media
• Use of CEHRT & compliance with HIPAA Security Rule (w/ONC)
• Enforcement process
• Update of existing FAQs to account for Omnibus and other recent developments
• Minimum necessary
HIPAA COMPLIANCE AUDITS
PHASE 2
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)

• Learn from this next phase in structuring permanent audit program

• Develop tools and guidance for industry self-evaluation and breach prevention
Program Status

• Desk audits underway
  ✓ 166 Covered Entities
  ✓ 45 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 Audit Phishing Scam – November 2016

Audit Phase 2

Alert: Phishing Email Disguised as Official OCR Audit Communication – November 28, 2016

It has come to our attention that a phishing email is being circulated on mock HHS Departmental letterhead under the signature of OCR’s Director, Jocelyn Samuels. This email appears to be an official government communication, and targets employees of HIPAA covered entities and their business associates. The email prompts recipients to click a link regarding possible inclusion in the HIPAA Privacy, Security, and Breach Rules Audit Program. The link directs individuals to a non-governmental website marketing a firm’s cybersecurity services. In no way is this firm associated with the U.S. Department of Health and Human Services or the Office for Civil Rights. We take the unauthorized use of this material by this firm very seriously.

OCR would like to further share that this phishing email originates from the email address OCRAudit@health.gov and directs individuals to a URL at http://www.health.gov.us. This is a subtle difference from the official email address for our HIPAA audit program, OCRAudit@health.gov, but such subtlety is typical in phishing scams.

Covered entities and business associates should alert their employees of this issue and take note that official communications regarding the HIPAA audit program are sent to selected auditees from the email address OCRAudit@health.gov. In the event that you or your organization has a question as to whether it has received an official communication from our agency regarding a HIPAA audit, please contact us via email at OCRAudit@health.gov

New Guidance for 2016 Desk Audits

- Selected Protocol Elements with associated document submission requests and related FAQs - PDF
- Slides from audited entity webinar held July 13, 2016 - PDF
- Comprehensive question and answer listing - PDF
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

Under OCR’s separate, broad authority to open compliance reviews, OCR could decide to open a separate compliance review in a circumstance where significant threats to the privacy and security of PHI are revealed through the audit.
## Covered Entity Desk Audit Controls

| Privacy Rule Controls | Notice of Privacy Practices & Content Requirements  
[§164.520(a)(1) & (b)(1)] |
|-----------------------|-----------------------------------------------------|
|                       | Provision of Notice – Electronic Notice  
[§164.520(c)(3)] |
|                       | Right to Access  
[§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)] |
| Breach Notification | Timeliness of Notification  
[§164.404(b)] |
| Rule Controls         | Content of Notification  
[§164.404(c)(1)] |
| 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

<table>
<thead>
<tr>
<th>Breach Notification Rule Controls</th>
<th>Notification by a Business Associate [§164.410, with reference to Content of Notification §164.404(c)(1)]</th>
</tr>
</thead>
</table>
## Audit Guidance

<table>
<thead>
<tr>
<th>Selected protocol elements with associated document submission requests and related Q&amp;As</th>
<th>Slides from audited entity webinar held July 13, 2016</th>
<th>Comprehensive question and answer listing</th>
</tr>
</thead>
</table>

OCR Website:  
http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html
COMPLIANCE, ENFORCEMENT & CYBERSECURITY
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.
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://scap.nist.gov/hipaa/
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
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:
  o Router and firewall firmware
  o Anti-virus and anti-malware software
  o 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).
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 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).
2016 - 2017 Enforcement Actions

• HIPAA settlement demonstrates importance of implementing safeguards for ePHI - January 18, 2017
• First HIPAA enforcement action for lack of timely breach notification settles for $475,000 – January 9, 2017
• UMass settles potential HIPAA violations following malware infection – November 22, 2016
• $2.14 million HIPAA settlement underscores importance of managing security risk – October 17, 2016
• 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
Cybersecurity

• 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
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

Electronic Secure Data, Enhanced Communication
Questions

• [http://www.hhs.gov/hipaa](http://www.hhs.gov/hipaa)
• Join us on Twitter @hhsocr
• Please complete an online session evaluation