HIPAA Updates from OCR

Evelyn Zeller, J.D.
evelyn.zeller@hhs.gov

Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

Health Care Compliance Conference
Seattle, WA June 9, 2017

OCR Update Topics

- Individual access to PHI – guidance issued
- Working in the cloud – guidance issued
- OCR’s audits
- Frequent compliance issues
- Recent enforcement examples
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

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Access – Scope

• Designated record set broadly includes medical, payment, and other records used to make decisions about the individual
  – Doesn’t matter how old the PHI is, where it is kept, or where it originated
  – Includes clinical laboratory test reports and underlying information (including genomic information)
Access – Scope (cont.)

- Very limited exclusions and grounds for denial
  - E.g., psychotherapy notes, information compiled for litigation, records not used to make decisions about individuals (e.g., certain business records) BUT underlying information remains accessible
  - Covered entity may not require individual to provide rationale for request or deny based on rationale offered
  - No denial for failure to pay for health care services
  - Concerns that individual may not understand or be upset by the PHI not sufficient to deny access

Access – Requests for Access

- Covered entity may require written request
- Can be electronic
- Reasonable steps to verify identity
- **BUT** cannot create barrier to or unreasonably delay access
  - E.g., cannot require individual to make separate trip to office to request access
  - Cannot require individual to complete an authorization form
Access – Form and Format and Manner of Access

• Individual has right to copy in form and format requested if “readily producible”
  – If PHI maintained electronically, at least one type of electronic format must be accessible by individual
  – Depends on capabilities, not willingness
  – Includes requested mode of transmission/transfer of copy
    • Right to copy by e-mail (or mail), including unsecure e-mail if requested by individual (plus light warning about security risks)
    • Other modes if within capabilities of entity and mode would not present unacceptable security risks to PHI on entity’s systems

Access – Timeliness and Fees

• Access must be provided within 30 days (one 30-day extension permitted) BUT expectation that entities can respond much sooner

• Limited fees may be charged for copy
  – Reasonable, cost-based fee for labor for copying (and creating summary or explanation, if applicable); costs for supplies and postage
  – No search and retrieval or other costs, even if authorized by State law
  – Entities strongly encouraged to provide free copies
  – Must inform individual in advance of approximate fee
No Fees Permitted for:

- Providing access through certified EHR technology (*i.e.*, View, Download, Transmit)
- Administrative overhead costs for outsourcing access requests to a business associate
- Viewing and inspecting PHI only

Third Party Access to an Individual’s PHI

- Individual’s right of access includes directing a covered entity to transmit PHI directly to another person, in writing, signed, designating the person and where to send a copy (45 CFR 164.524 – individual access)
- Individual may also **authorize** disclosures to third parties, whereby third parties initiate a request for the PHI on their own behalf if certain conditions are met (45 CFR 164.508 - authorization)
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.

Cloud Computing Guidance - continued

- 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.


OCR’s HITECH Audit Program

- Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; 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)
  - Also hope to learn from this next phase in structuring permanent audit program

History

- HITECH legislation: HHS (OCR) shall provide for periodic audits to ensure that covered entities and business associates comply with HIPAA regulations. (Section 13411)
  - Pilot phase (2011-2012) – comprehensive, on-site audits of 115 covered entities.
  - 2013 – issuance of formal evaluation report
  - 2016 – Phase 2 (ongoing) – between 200-250 onsite and “desk” audits of covered entities and business
Audit Program Status

- Desk audits underway
  - 166 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

Selected Desk Audit Provisions

- For Covered Entities:
  - Security Rule: risk analysis and risk management;
  - Breach Notification Rule: content and timeliness of notifications; or
  - Privacy Rule: NPP and individual access right

- For Business Associates:
  - Security Rule: risk analysis and risk management and
  - Breach Notification Rule: reporting to covered entity

- See protocol on-line for details:
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

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning
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

Enforcement Overview

- 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
  - 47 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 civil money penalties

As of April 30, 2017
2017 Enforcement Actions

- Memorial Hermann Health System
- CardioNet
- Center for Children’s Digestive Health
- Metro Community Provider Network
- Memorial Healthcare System
- Children’s Medical Center of Dallas
- MAPFRE Life Insurance Company of Puerto Rico

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
Resources - OCR Cybersecurity Newsletters

- February 2016 (Ransomware, “Tech Support” Scam, New BBB Scam Tracker)
- March 2016 (Tips for keeping PHI safe, NSA’s lessons learned, 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)

Resources - OCR Cybersecurity Newsletters - continued

- October 2016 (Mining More than Gold)
- November 2016 (What Type of Authentication is Right for you?)
- December 2016 (Understanding DoS and DDoS Attacks and Best Practices for Prevention)
- January 2017 (Understanding the Importance of Audit Controls)
- February 2017 (Reporting and Monitoring Cyber Threats)
- April 2017 (Man-in-the-Middle Attacks and “HTTPS Inspection Products”)
Questions?

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr