Update on Administration and Enforcement of the HIPAA Privacy, Security, and Breach Notification Rules

Wandah Hardy, Rn. BSN, MPA
Equal Opportunity Specialist/Investigator
Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

Updates

• Policy Development
• Breach Notification
• Enforcement
• Audit
POLICY DEVELOPMENT

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
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

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

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 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)
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
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.


Cybersecurity Newsletters

- February 2, 2016 (Ransomware, “Tech Support” Scam, New BBB Scam Tracker)
- March 3, 2016 (Tips for keeping PHI safe, NSA's lessons learned, Malware and Medical Devices)
- March 30, 2016 (New Cyber Threats and Attacks on the Healthcare Sector)
- May 3, 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?)

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.


Policy Development – What’s Coming

- Guidance on text messaging
- Social media guidance
- PMI and research authorizations
- 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
BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

Breach Notification Requirements

- 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
September 2009 through February 28, 2017

- Approximately 1,849 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 50% of large breaches
  - Hacking/IT now account for 15% of incidents
  - Laptops and other portable storage devices account for 28% of large breaches
  - Paper records are 22% of large breaches
  - Individuals affected are approximately 171,569,574

- Approximately 279,157 reports of breaches of PHI affecting fewer than 500 individuals
HIPAA Breach Highlights

500+ Breaches by Location of Breach as of February 28, 2017

- Desktop Computer: 11%
- Laptop: 18%
- Portable Electronic Device: 9%
- Network Server: 16%
- Email: 9%
- EMR: 6%
- Paper Records: 22%

What Happens When HHS/OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - 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
• Over 150,507 complaints received to date
• Over 24,879 cases resolved with corrective action and/or technical assistance
• Expect to receive 17,000 complaints this year

As of 2/28/2017

• 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
  – 44 settlement agreements that include detailed corrective action plans and monetary settlement amounts
• 3 civil money penalties

As of February 28, 2017
**2017 Enforcement Actions**

- Memorial Healthcare System
- Children’s Medical Center of Dallas
- MAPFRE Life Insurance Company of Puerto Rico
- Presence Health
- University of Massachusetts Amherst
- St. Joseph Health

**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
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 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

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:
Status

• 167 Covered entity desk audits underway; desk audits of business associates to begin in November.

• On-site audits will begin in 2017.
  – On-site audits will evaluate auditees against comprehensive selection of controls in the audit protocol:
    http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/

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