Individual Access, Audit, & Enforcement Updates

2016 HCCA Conference
October 13, 2016

Presentation Overview

- Office for Civil Rights (OCR)
  - Who we are
  - OCR's Pacific Region
- Individual Access
  - Access Requests Directed to a Third Party
  - Electronic Access Guidance
- OCR Audit
  - Updates
  - What to expect
- Policy Development
- Breach Highlights & Enforcement Activity

2

Office for Civil Rights (OCR)

- Part of the U.S. Department of Health and Human Services
- Enforces the HIPAA Privacy, Security, and Breach Notification Rules
- Enforces a number of civil rights laws as they relate to recipients of Federal financial assistance (FFA) from HHS, public entities, and programs & activities conducted by HHS
- Headquartered in D.C. with 8 regional offices (in 11 locations) across the U.S.

3

Regional Map

4

Office for Civil Rights

Pacific Region covers the following states:

- Alaska
- Arizona
- California
- Hawaii
- Idaho
- Nevada
- Oregon
- Washington
- U.S. Pacific Territories

5

Individual Access

6

Privacy Updates: Overview

- Access Guidance
  - Access Requests Directed to Third Parties
  - Requests for Electronic Copies
  - Fees

7

Right of Access

An individual has the right, if requested,
to inspect and obtain a copy (or both)
of his/her PHI maintained in one or more designated record sets by a covered entity
with limited exceptions

Includes the right to direct the covered entity to **send a copy to a designated person or entity of the individual's choice**

45 CFR 164.524
45 CFR 164.524(c)(3)(ii)

8

Directed to Third Parties

- If requested by the individual, CE must transmit copy of PHI to individual's designee
  - Request must be in writing
  - Must be signed by the individual and
  - Must clearly identify designated person and where to send the PHI
- CE must still verify identity of individual making request

45 CFR 164.524(c)(3)(ii)

9

Directed to Third Parties cont.

- Same access requirements apply to requests directed to third parties
  - Fee limits
  - Time limits
  - Denials, etc.
- If the nature of the request is unclear, the CE may seek clarification from the individual
- Third party liability limits

10

Authorization vs. Access

HIPAA Authorization

- CE permitted to disclose
- Specific required elements
- No deadline for disclosure
- Reasonable safeguards
- No limits on fees, except sale of PHI must be disclosed.

Right of Access

- CE required to disclose
- Signed request
- 30 day deadline to respond
- Reasonable safeguards, with exceptions
- Fee limits, same as for individual access

11

Requests for Electronic Copies

Paper PHI

- CE's must provide electronic copy of PHI, if readily producible, and in form and format requested, if readily producible in that format
- If NOT readily producible in format requested, in an alternative electronic OR hard copy format, as agreed to by the CE and the individual

Electronic PHI

- CE's must provide copy of ePHI electronically, and in the form or format requested, if readily producible in that format
- If NOT readily producible in format requested, then in an alternative electronic format, as agreed to by the CE and the individual

12

Fees for Copies: Reasonable & Cost-Based

Includes:

- Labor for copying PHI
- Supplies for creating copy
- Postage, if mailed
- Preparation of explanation or summary, if individual agrees

Does not include:

- Verification
- Documentation
- Search/retrieval
- Maintaining systems
- Recouping capital
- Other costs

* Even if authorized by state law

13

Other Impermissible Fees

- Fees also NOT 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

14

Access Fees and State Law

- Access fees authorized by state law may be charged only if they are:
  - Cost-based expenses of the same types that HIPAA permits (*e.g.,* labor for copying, supplies & postage)
  - Reasonable (*e.g.,* not higher than the CE's actual cost)
- State laws that allow only lesser fees than what HIPAA allows remain effective (including state law requirements to provide free records to individuals)

15

Calculating Costs for Access Fees

1. Actual costs
   - Actual labor for copying (at reasonable rates, including only the time to create and send a copy in the form, format, and manner requested)
   - Actual postage
   - Supplies (paper, toner, CD, USB drive)
2. Average costs
   - Cost schedule based on average labor costs for standard requests is okay
   - Per page fee acceptable only for paper records (copied or scanned)
   - Applicable supply and postage costs may be added to average labor costs
3. Flat fee for electronic copies of electronic PHI only ($6.50 cap)

16

Advance Notice of Access Fees

- CEs must provide individuals with advance notice of fees to be charged with information about form, format, and manner costs.
  - Fee information must be provided at the time the access is requested (or when form, format, and manner are negotiated)
  - Access fee schedules should be posted online
  - CEs should provide itemized listing of charges for labor, supplies, and postage, upon request
- Labor costs for preparing an explanation or summary of PHI must be provided in advance by the CE and agreed to by the individual.

17

Right to View and Inspect PHI

- Covered entities must have reasonable procedures for individuals to arrange a convenient time and place to inspect PHI.
- Fee may not be charged to the individual
- While inspecting PHI, individuals may (without charge):
  - Take notes
  - Take pictures of the PHI
  - Use other personal resources to capture the information.
- CEs may have reasonable policies to safeguard information and protect privacy and security and avoid disruptions during inspection.

18

Audits

19

Audits Overview

- Phase 1
- Phase 2
  - Update
  - Selection Process
  - Protocol Criteria & Scope
  - Timeline
  - Expectations
- Recent Updates & Resources

20

Audits Mandated

HITECH Act, Section 13411 – Program Mandate

- Requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the Privacy and Security Rules and Breach Notification Standards

Program Opportunity

- Examine mechanisms for compliance
- Identify best practices
- Discover risks and vulnerabilities not surface through complaint investigations and compliance reviews

21

Phase 1 Completed

- Audit Pilot
  - Completed December 2012
  - 115 Covered Entities
    - Sample selection
- Pilot Process
  - On-site Audits
  - Published audit protocol
- Assessment

22

Phase 2 Update

- Includes covered entities **and** business associates
- 200-250 audits in total
  - Over 200 desk audits (underway)
  - Smaller number of comprehensive on-site audits (early 2017)
- Selection Process

Phase 2 Protocol Criteria

- Auditors will assess efforts through an updated protocol
- Updated protocol is available on web site

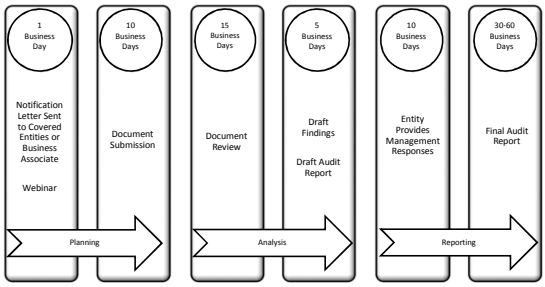
Audit Type	Section	Key Activity	Established Performance Criteria	Audit Inquiry	For Security only: Required/ Addressable
Privacy	§164.514 (d)(3)	Minimum Necessary - Disclosures of PHI	§164.514(d)(3) Implementation specification: Minimum necessary disclosures of protected health information. (i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure...	Are policies and procedures in place to limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure? Obtain and review policies and procedures related to minimum necessary disclosures and evaluate the content relative to the established performance criterion. Obtain and review a sample of protocols for disclosures made on a routine and recurring basis and determine if such protocols limit to the PHI to what is reasonably necessary to achieve the purpose of the disclosure, as required by 514(d)(3).	

Scope (Desk Audits)

- Covered Entities
  - Security – risk analysis and risk management
  - Breach – content and timeliness of notifications
  - Privacy – notice and access
- Business Associates
  - Security – risk analysis and risk management
  - Breach – reporting to covered entities

25

Audit Process (Desk Audits)



26

Desk Audit Expectations

- 10 business days to respond
- Provide specified documentation – applicable policies, procedures, evidence of implementation
- Provide complete and relevant materials
- Refrain from submitting extraneous documentation
  - 10 MB file size limit

27

Resources

Website:

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

Audit Mailbox:

OSOCRAudit@hhs.gov

28

Policy Development

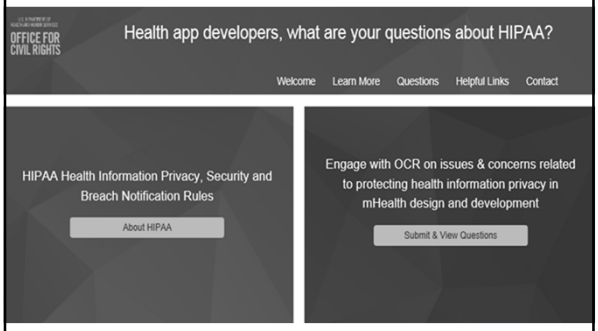
29

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
  - http://hipaaQsportal.hhs.gov/
- 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

30

HIT Developer Portal



31

Policy Development - Updates

- Cloud guidance - Published October 7, 2016
- 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

32

Breach Highlights & Enforcement Activity

33

Breach Notification

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

34

HIPAA Breach Highlights

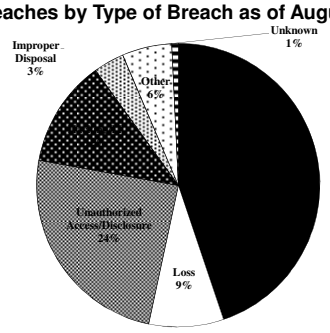
September 2009 through August 31, 2016

- Approximately 1,652 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 54% of large breaches
  - Hacking/IT now account for 12% of incidents
  - Laptops and other portable storage devices account for 29% of large breaches
  - Paper records are 22% of large breaches
  - Individuals affected are approximately 168,256,575
- Approximately 236,944 reports of breaches of PHI affecting fewer than 500 individuals

35

HIPAA Breach Highlights

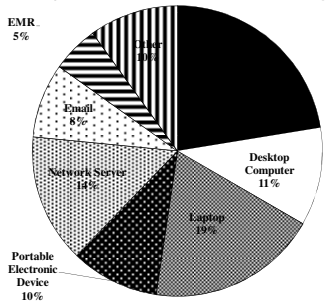
500+ Breaches by Type of Breach as of August 31, 2016



36

HIPAA Breach Highlights

500+ Breaches by Location of Breach as of August 31, 2016



37

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

38

General Enforcement Highlights

- Over 139,864 complaints received to date
- Approximately 1,098 compliance reviews initiated
- Over 24,424 cases resolved with corrective action and/or technical assistance
- Expect to receive 17,000 complaints this year

39

General Enforcement Highlights

- 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
  - 36 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 2 civil money penalties

40

Recurring Compliance Issues

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

41

Corrective Action

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

42

Risk Analysis Tips

Risk Analysis: Assessment of potential threats and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

- **Vulnerabilities**- are internal flaws or weaknesses in current safeguards (security measures and policies and procedures) that, if accidentally triggered or intentionally exploited by a threat, could result in a security incident.
- **Threats-** persons or things that can accidentally trigger or intentionally exploit vulnerabilities.

43

Identify and Document Vulnerabilities

Technical Vulnerabilities:

- Unsupported software (e.g., Windows XP free/open-source)
- Software is not patched or regularly updated
- Antivirus software is not set to automatically scan
- Antivirus or intrusion detection system signatures are not regularly updated
- Network security devices are not properly configured or used
- Users with excessive rights, privileges, or access
- Generic user accounts (no accountability
- Easily guessed or cracked passwords
- Insufficient audit controls
- Unauthorized servers, workstations, devices, applications, ports, protocols
- No or insufficient encryption solutions (e.g., DES, WEP)
- No or insufficient integrity mechanisms

Non-technical Vulnerabilities:

- Policies and procedures are not sufficient (e.g., no backup plan)
- Insufficient training
- Insufficient physical safeguards (e.g., workstation cable locks, fire extinguishers)

44

Identify and Document Reasonably Anticipated Threats

Human Threats:

- Cyber-attack
- Social Engineering (manipulating people to obtain technical or physical access)
- Interception and/or alteration of e-PHI being transmitted
- Attacker or unsuspecting workforce member injects malicious software into or downloads e-PHI from the information system using a portable device (e.g., USB thumb drive)
- Attacker guesses a password
- Theft
- Loss
- Destruction
- workforce member impermissibly uses or discloses e-PHI

Natural Threats:

- Earthquake/Hurricane/ Tornado/Tsunami
- Fire/Flood

Environmental Threats

- Power Failure
- Temperature or humidity change that affects the information network

45

Risk Analysis

- Confidentiality is impacted if e-PHI is available to or disclosed to unauthorized persons or processes.
- Integrity is impacted if e-PHI is altered or destroyed in an unauthorized manner.
- Availability is impacted if e-PHI is not accessible or is not useable by authorized persons on demand.

46

"Reasonably Anticipated": Unique to Each Organization

Organizational Factors
- Size
- Type
- Complexity
- Resources
- Infrastructure
- Existing Policies
- Cost of Security Measures
- Human Element
  - Error
  - Intent

External Factors
- Natural environment
- Infrastructure
- Human Element
  - Intent

47

Determine Level of Risk: Likelihood + Impact = Risk

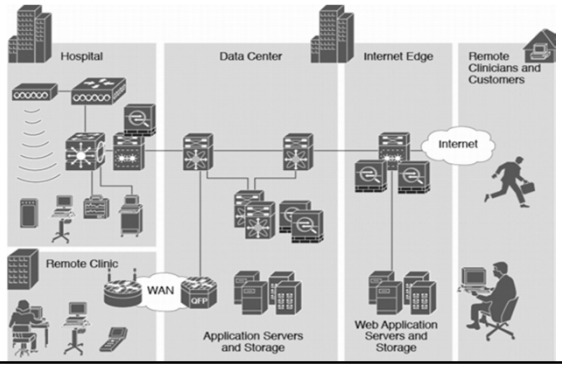
Level of risk is a function of: (1) the likelihood of a particular threat triggering or exploiting one or more vulnerabilities; and (2) the potential impacts to confidentiality, integrity, and availability of e-PHI.

Threat Source	Vulnerabilities	Threat Level	C Impact	I Impact	A Impact	Risk Level
Theft	No encryption, no cable lock	High	High	High	High	High
Current WFM impermissible use or disclosure	excessive rights, privileges, or access; no accountability (audit and review)	Medium	High	High	Low	Medium

Threat Agent	Threat Action	Vulnerability	Risk Likelihood	Risk Impact	Risk Rating
Network Connectivity Outage	Loss of Internet connectivity	Vulnerabilities related to telecommunications providers	5	4	20
Careless IT personnel	Insecure configuration of systems	Vulnerabilities in system configurations	5	4	20

48

Scope: Enterprise Wide



Risk Analysis vs. "Gap Assessment"

Rule/Section		Gap	Security Manager Program (WBS 1	Business Continu Disaster Recovery 2.0)	Policies and Proce (WBS 3.0)	Human Resourc Procedures (WBS	Business Associ Agreements (WBS	Training/Awarenes 6.0)	Technical Archite (WBS 7.0)	Evaluation (WBS	System/Netwo Management (WS	User Management 10.0)
Administrative Safeguards												
164.308(a)(1)	Security Management Process	◆	✓		✓	✓						
164.308(a)(2)	Assigned Security Responsibility	○			✓	✓						
164.308(a)(3)	Workforce Security	◆	✓		✓	✓						
164.308(a)(4)	Information Access Management	◆	✓		✓							✓
164.308(a)(5)	Security Awareness and Training	◆	✓		✓			✓				✓
164.308(a)(6)	Security Incident Procedures	○										
164.308(a)(7)	Contingency Plan	◆		✓	✓			✓				
164.308(a)(8)	Evaluation	◆	✓		✓					✓		
164.309(b)(1)	Business Associates Contracts	●					✓					
Physical Safeguards												
164.310(a)	Facility Access Control	◆	✓	✓	✓			✓				
164.310(b)	Workstation Use	●			✓							✓
164.310(c)	Workstation Security	●			✓							✓
164.310(d)	Device and Media Controls	○										
Technical Safeguards												
164.312(a)	Access Controls	◆							✓			✓
164.312(b)	Audit Controls	○										
164.312(c)	Integrity	◆							✓			
164.312(d)	Person or Entity Authentication	◆							✓			

50

Documentation and Periodic Review

51

Core Concepts to Remember

Risk Analysis is:

- Defining system characteristics & scope
- Identifying threats & vulnerabilities
- Assessing probability & criticality of potential risks
- Prioritizing risks
- Documenting rationales behind security decisions
- Periodic reassessment of security risks & controls

Risk Analysis is necessary for:

- Identifying reasonably anticipated risks
- Determining "reasonable and appropriate" security measures
- Implementing effective security measures
- Assessing & updating existing security measures

52

Good Practices

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

53

Enforcement Examples

- ***Oregon Health and Science University (6/2016) $2,700,000***
  - Laptop/thumb drive thefts
  - Take Away: Importance of conducting an enterprise-wide risk analysis
- ***University of Mississippi Medical Center (7/2016)* $2,750,000**
  - Laptop theft
  - Network drive vulnerable to unauthorized access
  - Take Away: Importance of identifying unaddressed risks and conducting an enterprise-wide risk analysis

54

On-Line Resources

- Learn more about OCR guidance and enforcement, and sign up for the OCR Privacy & Security Listserv: http://www.hhs.gov/hipaa/for-professionals/index.html
- Join us on Twitter @hhsocr
- Other resources:
  - https://www.healthit.gov/providers-professionals/ehr-privacy-security
  - http://www.nist.gov/information-technology-portal.cfm
  - https://www.sans.org/online-security-training/

55

Contact Us

OCR Website: http://www.hhs.gov/ocr

56