


Individual Access, Audit, & Enforcement Updates

2016 HCCA Conference
November 11, 2016



Presentation Overview

Office for Civil Rights (OCR)

- Who we are

Individual Access

- Access Requests Directed to a Third Party
- Electronic Access Guidance


OCR Audit

- Updates
- What to expect

Enforcement Updates

- Risk Assessment Tips
- Recent Enforcement Highlights

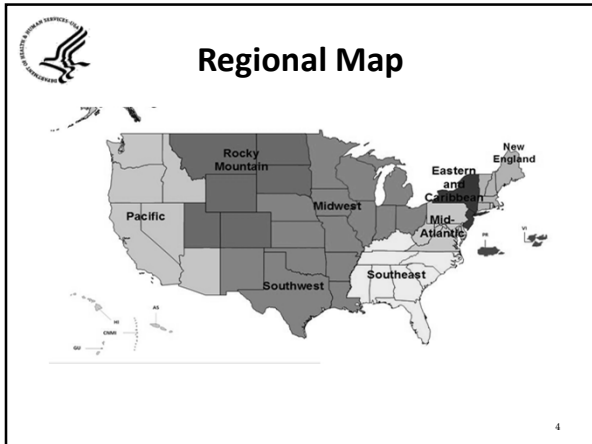
2



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







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/or obtain a copy 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, the 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
- The 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

<p><u>HIPAA Authorization</u></p> <ul style="list-style-type: none"> • CE permitted to disclose • Specific required elements • No deadline for disclosure • Reasonable safeguards • No limits on fees, except sale of PHI must be disclosed. 	<p><u>Right of Access</u></p> <ul style="list-style-type: none"> • 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

- CE's must provide an electronic copy of PHI, if it is readily producible in the form and format requested
- If it is NOT readily producible in format requested, the CE must provide it in an alternative electronic OR hard copy 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 a 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 the following:
 - 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

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.
- A 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
- 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 at www.HHS.gov/OCR

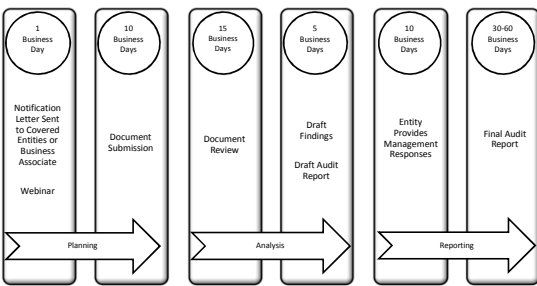
Audit Type	Section	Key Activity	Established Performance Criteria	Audit Inquiry	For Security only: Required/Addressable
Privacy	§164.514 (d)(3)	Minimum Necessary Disclosures of PHI	§164.514(d)(3) Implementation specification: Minimum necessary disclosures of protected health information. (i) For any type 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 §14(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



Enforcement Updates

29

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.

30

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)

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

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.

“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

34

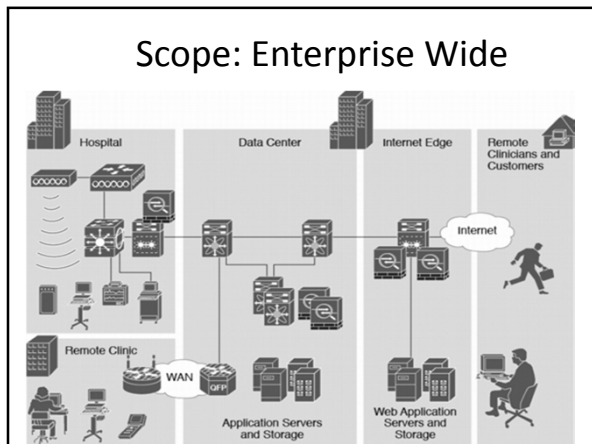
Determine Level of Risk: Likelihood + Impact = Risk

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 WEM 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

35



Enforcement Examples

- **Cancer Care Group, P.C. (9/2015) \$750,000**
 - Theft of laptop and unencrypted backup media
 - **Take Away:** Importance of conducting Risk Analysis, including Mobile Device Security
- **Oregon Health and Science University (6/2016) \$2.7M**
 - Theft of laptop/thumb drive
 - **Take Away:** Importance of conducting an enterprise-wide risk analysis

40

On-Line Resources

- <http://www.hhs.gov/hipaa/for-professionals/index.html>
- <https://www.healthit.gov/providers-professionals/ehr-privacy-security>
- <http://www.nist.gov/information-technology-portal.cfm>
- <https://www.sans.org/online-security-training/>

41

Contact Us

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

42
