

**Getting OCR Audit-Ready in
7 Steps:**

Kimberly B. Holmes, Esq.
Senior Vice President & Counsel
Cyber Insurance, Liability & Emerging
Risks
March 28, 2017



Remember first of all... 

Pursuant to the *HIPAA Security Rule provision on Audit Controls*, 45 C.F.R. sec.164.321(b):

- Covered Entities and Business Associates *must implement hardware, software and/or processes that both record and review activity in IT systems containing or using electronic PHI.*

Audit Insight from the recent OCR Enforcement Landscape 

- Among Others in 2016:
 - University of Mississippi Medical Center
 - Oregon Health & Science University
 - \$2.7M CMP imposed against each CE
 - *Failure to act on identified problems/risks*
- Already in 2017:
 - 3 Major CMP Cases
 - Presence Health Network (\$475k), Children’s Hospital of Dallas (\$3.2M CMP imposed), *Memorial Health Care System (\$5.5M)*

An Audit Roadmap to Learn From...
Memorial Health Care System (2/16/17)



OCR Findings:

- Impermissible disclosure of PHI in violation of the Privacy Rule
- Failure to implement procedures to *regularly* review records of information system activity such as audit logs
- Failure to implement policies and procedures to *review and modify* users' access to PHI.

OCR Audit Control Guidance (Jan. 2017)



- Secure Audit Logs & Audit Trails
 - Audit Logs: Records of events based on applications, users, systems (NIST)
 - Audit Trails: Maintain a record of system activity by application and user activity (NIST)
- Use "reasonable and appropriate" tools to collect, monitor and review* audit controls
 - * Restrict review access; need-to-know basis only

OCR Audit Control Guidance (Jan. 2017)
(Cont'd)



- Lack of access controls and failure to regularly review audit logs enables hackers and wrongdoing insiders to cover their tracks
- Implementing audit controls and reviewing audit logs *regularly*:
 - Facilitates easier recovery from breaches
 - May help prevent them from happening in the first place

Types of Audit Trails



Application

- Monitors and logs user activities; when data files are opened/closed, created, read, edited or deleted

System-level

- Tracks successful/unsuccessful log-on efforts; and what application the user was seeking to access

User

- Monitors user activity by tracking events user initiates (log-on attempts, access to files, etc.)

7-Steps to OCR Audit-Readiness



- Gather your Team (in-house, external resources as needed (i.e, Privacy/HIPAA Counsel, Forensics)
- Determine "Reasonable and Appropriate" Audit Controls to be Implemented
- Conduct/Update enterprise-wide Risk Analysis/Risk Assessment of security risks/weaknesses
 - Understand first what PHI and Tech/IT inventory/assets you actually have

7-Steps to OCR Audit-Readiness (Cont'd)



- Implement or Review enterprise-wide Risk Management Plan (to address identified risks/gaps/weaknesses)
 - Implement/Enforce/Test/Revise as Needed
 - Document, Document, Document
 - Rationale for Resource Allocation/Plan for Addressing Non-Compliance where Applicable
- Review/Revise Policies & Procedures As Needed for:
 - Information systems activity review;
 - Establishing, modifying and terminating access
- Provide Workforce Training
- Regularly review ALL of the above in *normal course of business*

What are “Reasonable and Appropriate” Audit Controls? 

- Consider Your Risk Analysis results as well as current:
 - Infrastructure
 - Hardware and software security capabilities
- Commensurate with available financial and human resources
- What your Policies & Procedures can support

4-Factor Risk Assessment 

- Identify your risks/vulnerabilities
- Determine remediation steps needed
- Allocate Resources to address; Outline a rationale (and plan) where not currently addressing a particular risk/vulnerability
- TAKE ACTION to address the risks identified
 - Identified risks/vulnerabilities set the FLOOR of remediation responsibility
 - Clock is ticking from this point...until an event occurs
 - Don't wait to address
 - At minimum: document when/what steps will be taken for all identified risks

Be Aware of OCR's past hot buttons... 

- Implement robust physical safeguards
 - No unrestricted access to unauthorized individuals
 - Implement Access Controls & Device/Media Controls
- Encrypt and password-protect all points of data access
 - Not required, but consider at minimum:
 - Document reasons for current status if not fully encrypted as Risk Analysis/Assessment will likely point to risks of unencrypted PHI
- Implement/Distribute & Enforce a mobile device policy



QUESTIONS?

kimberly.holmes@idexpertscorp.com
