How to Conduct an OCR-Quality® Risk Analysis

Jon Moore | MS, JD, HCISPP

Chief Risk Officer and Head of Consulting Services and Client Success

Clearwater

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Agenda

- The Problem with Risk Analysis
- The Requirement
- OCR’s Guidance
- Audit Criteria
- Additional Resources

Today's Presenter

Jon Moore, MS, JD, HCISPP

Chief Risk Officer and Head of Consulting Services and Client Success

- 25+ years Executive Leadership, Technology Consulting and Law
- 14+ years Data Privacy & Security
- 10+ years Healthcare
- Former PwC Federal Healthcare Leadership Team
- Former IT Operational Leader PwC Federal Practice
- BA Economics Haverford College, MS E-Commerce Carnegie Mellon University, JD Dickinson Law Penn Stat University
- Architect of Federal IT GRC Solution
- Expertise and Focus: Healthcare, Risk Management, Compliance
- Speaker and Published Author on Security, Privacy, IT Strategy and Impact of Emerging Technologies

https://www.linkedin.com/in/jonamoore/

Organizations Struggle with Risk Analysis

OCR enforcement and audit results demonstrate that covered entities and business associates struggle with the risk analysis requirement of the HIPAA Security Rule.

90%

Of OCR ePHI-related enforcement actions found failure to conduct risk analysis.

- Not detailed or comprehensive enough
- Not following OCR guidance
- Not enough documentation/evidence

14%

Of covered entities audited by OCR substantially fulfilled their regulatory responsibility to conduct risk analysis.

17%

Of business associates audited by OCR substantially fulfilled their regulatory responsibility to conduct risk analysis.

Clearwater

https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf

Reasonable and Appropriate Safeguards

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

45 C.F.R. § 164.306(a)
Specifically

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce

45 C.F.R. § 164.306(b)(2)
Considerations for Organization

1. Its size, complexity, and capabilities,
2. Its technical, hardware, and software infrastructure,
3. The costs of security measures, and
4. The likelihood and possible impact of potential risks to e-PHI.6

The Risk Analysis Requirement

Risk analysis is a required administrative safeguard under 45 CFR §164.308.

§ 164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with §164.306:

(1) (i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

OCR's Guidance on Risk Analysis

On July 14, 2010, OCR issued Guidance on Risk Analysis Requirements under the HIPAA Security Rule.

Elements a risk analysis must incorporate:

1. Scope of Analysis
2. Data Collection
3. Identify and Document Potential Threats and Vulnerabilities
4. Assess Current Security Measures
5. Determine the Likelihood of Threat Occurrence
6. Determine the Potential Impact of Threat Occurrence
7. Determine the Level of Risk
8. Finalize Documentation
9. Periodic Reviews and Updates to the Risk Analysis

" There are numerous methods of performing risk analysis and there is no single method or 'best practice' that guarantees compliance with the Security Rule. Some examples of steps that might be applied in a risk analysis process are outlined in NIST SP 800-30."

What Does Not Qualify as Risk Analysis

In April 2018 OCR published a newsletter, Risk Analyses vs. Gap Analyses- What is the Difference?, specifically calling out that risk analysis is not the same as a gap assessment or analysis.

Security Controls Gap Analysis

A Security Controls Gap Assessment is a systematic process used to evaluate the effectiveness of an organization's existing security controls compared to a set of industry standards, best practices, or regulatory requirements.

Example standards: NIST CSF, CIS Top 18, ISO 27001.

Compliance Gap Analysis

A Compliance Gap Assessment is a detailed evaluation aimed at determining the extent to which an organization's practices, procedures, and controls align with specific regulatory requirements or industry standards.

Example regulatory requirements: HIPAA Security Rule, GDPR, PCI, HITRUST

Some Definitions

Important terms not defined in Security Rule that are defined in the OCR's Guidance on Risk Analysis.

Vulnerability

"[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy." NIST SP 800-30

Threat

"[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." Adapted from NIST SP 800-30. Includes natural (i.e. weather, earthquakes), human (intentional and unintentional) and environmental threats (i.e. power outages, water leaks, chemicals).

Risk

"The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur . . . . " Adapted from NIST SP 800-30

From Where do Risks Arise?

Risks arise from legal liability or mission loss as a result of four primary reasons.

1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
2. Unintentional errors and omissions
3. IT disruptions due to natural or man-made disasters
4. Failure to exercise due care and diligence in the implementation and operation of the IT system.

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

Scope of the Analysis

An organizations risk analysis should consider all its ePHI regardless of the electronic medium in which it is created, received, maintained or transmitted. (45 C.F.R. § 164.306(a))

Clinical Systems & Software

- Automated Medication or Medical Supply Cabinets
- Billing Information System
- Claims Payment System
- Clinical Workstations (e.g., Thin or Zero-client Computers, Portable Laptop Carts, etc.)
- Core Health Information System
- Diagnostic Equipment (e.g., EKG, EEG, Pulmonary Function Testing, etc.)
- Dictation devices
- Electronic Health Record System
- Emergency Department System
- Lab Information System
- ICU/NICU Telemetry System
- Oncology System
- Operating Room Software
- PACS System (Picture Archiving and Communication System)
- Patient Portal
- Radiology Information System
- Incident Management System
- Telehealth software
- Mobile patient apps

Equipment and Infrastructure

- Administrative Workstations (e.g., Desktop and Laptop Computers)
- Closed Circuit Television (CCTV) System
- Document Management System
- MS SharePoint
- Email System
- Fax System
- Network File Shares
- Document/Records Storage and Management Vendor
- Medical Equipment Maintenance Supplier
- Cloud Environment

Medical Devices

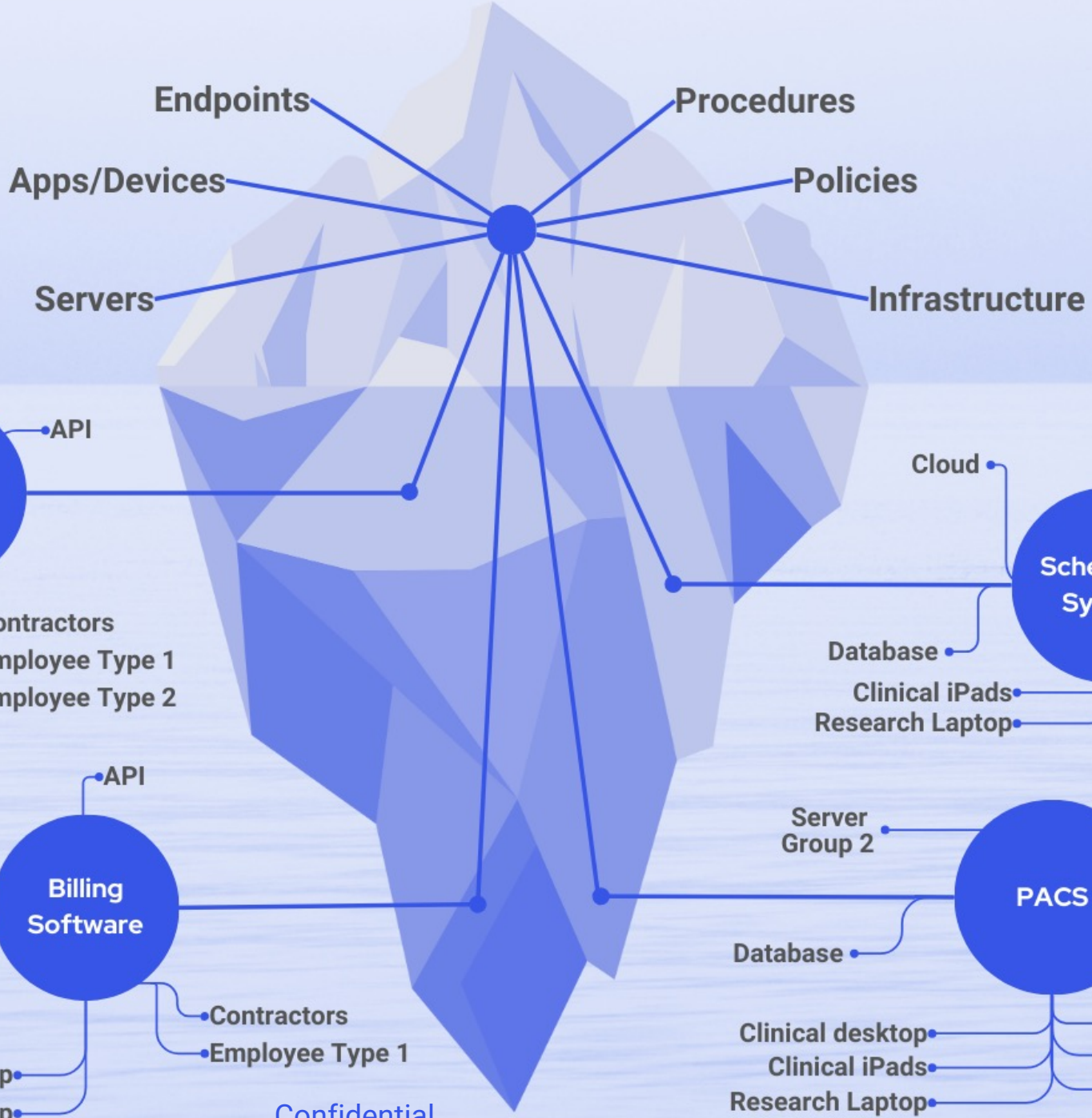
- Diagnostic Equipment (e.g., EKG, EEG, Pulmonary Function Testing)
- Laboratory Equipment (e.g., Hematology Analyzer, TEG devices)
- Radiological Equipment (e.g., CT, MRI, PET Scanners, Mammography, Ultrasound, X-ray Machines, Gamma Knife)
- Remote Monitoring Devices

Business Systems

- Financial System
- HR Systems

Traditional Risk Analysis

NIST Risk Management Tiers 1 & 2



Asset-Based Risk Analysis

NIST Risk Management Tier 3

Data Collection

An organization must identify where its ePHI is created, received, maintained or transmitted. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)

Methods to collect data:

- Reviewing past and/or existing projects
- Performing interviews
- Reviewing documentation
- CMDB system and software inventories
- Using other data gathering techniques

"The data on e-PHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)"

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

Identify and Document Potential Threats and Vulnerabilities

Organizations must identify all reasonably anticipated threats and vulnerabilities. (See 45 C.F.R. §§ 164.306(a)(2) , 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Example Threats

- Burglar/ Thief
- Electrical Incident
- Fire
- Flood
- Inclement weather
- Malware
- Ransomware
- Network Connectivity Outage
- Power Outage/Interruption

Example Vulnerabilities

- Anti-malware Vulnerabilities
- Destruction/Disposal Vulnerabilities
- Dormant Accounts
- Endpoint Leakage Vulnerabilities
- Excessive User Permissions
- Insecure Network Configuration
- Insecure Software Development Processes
- Insufficient Application Capacity
- Insufficient data backup

Assess Current Security Measures

Organizations should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

NIST SP 800-53A Rev 5 identifies three control assessment methods:

1. The **examine method** is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities) to facilitate assessor understanding, achieve clarification, or obtain evidence.
2. The **interview method** is the process of holding discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence.
3. The **test method** is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare the actual state of the object to the desired state or expected behavior of the object.

Examples of controls:

- PS-6 a The organization ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.
- PS-6 b The organization reviews/updates the access agreements [Assignment: organization-defined frequency].
- AC-19 a The organization establishes usage restrictions and implementation guidance for organization-controlled mobile devices.
- AC-19 d The organization enforces requirements for the connection of mobile devices to organizational information systems.

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

Determine the Likelihood of Threat Occurrence

Organizations need to consider the probability of potential risks to ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

How likely is it that a burglar will walk off with one of our administrative desktops given the physical controls, or lack there of, that we have in place?

How likely are we to lose access to the system due to a flood when the system is in the basement within a flood plain?

How likely is it that we will get malware on a clinical desktop if we don't have a vulnerability management program in place that patches them regularly?

"The output of this part should be **documentation of all threat and vulnerability combinations** with associated likelihood estimates that may impact the confidentiality, availability and integrity of e-PHI of an organization. (See 45 C.F.R. §§ 164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)"

Determine the Potential Impact of Threat Occurrence

Organizations need to consider the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

What is the potential impact to the organization if a burglar walks off with one of our administrative desktops given the physical controls, or lack there of, that we have in place?

What is the potential impact to the organization if we lose access to the system due to a flood?

What is the potential impact to the organization if we get malware on a clinical desktop because we don’t have a vulnerability management program in place that patches them regularly?

“The output of this part should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of e-PHI within an organization. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).) “

Determine the Level of Risk

Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

"The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)"

Finalize Documentation

Organizations must document their risk analysis. (See 45 C.F.R. § 164.316(b)(1).)

The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).)

- Contents:
- Where ePHI resides
- Threats
- Vulnerabilities
- Safeguards
- Likelihood of threat vulnerability combinations
- Impact of threat triggering vulnerability
- Risk levels and corrective actions

Periodic Review and Updates to the Risk Analysis

For organizations to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).)

Frequency:

“The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.”

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessment

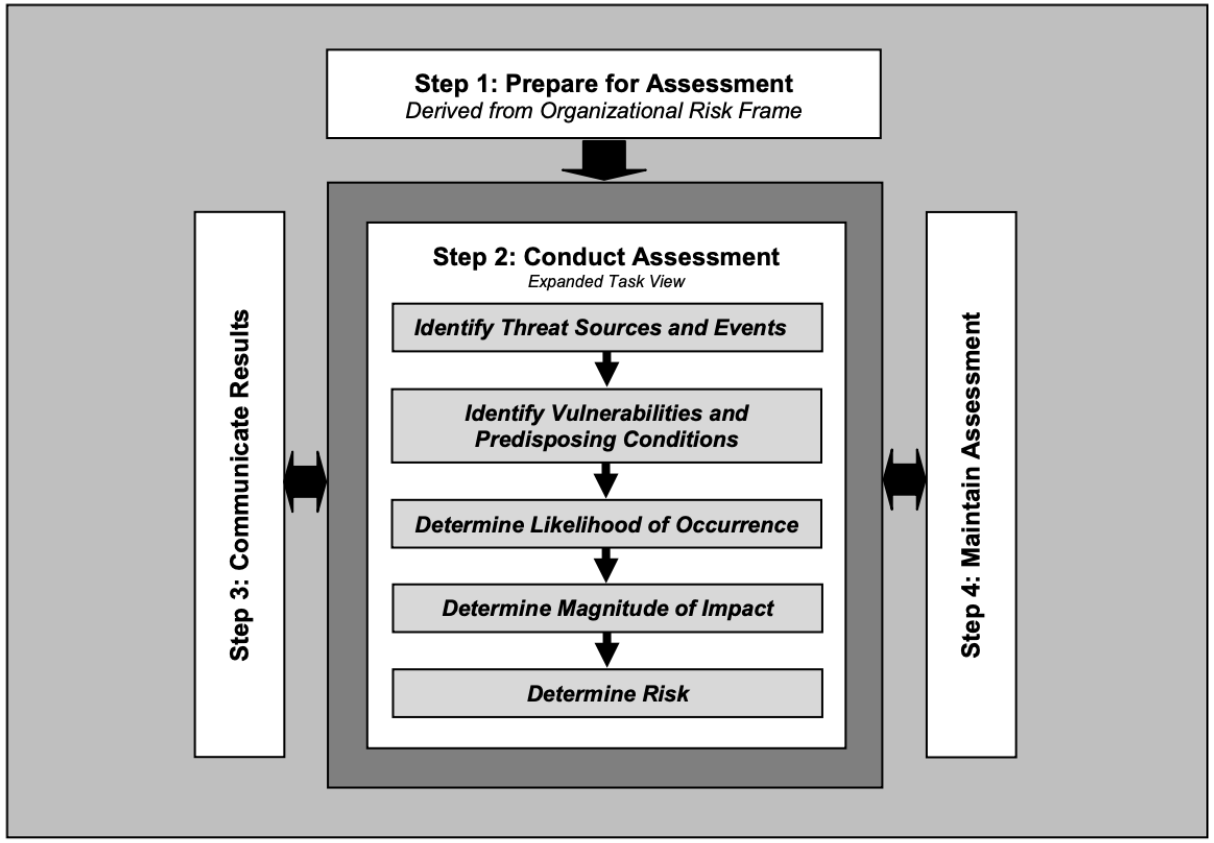


FIGURE 5: RISK ASSESSMENT PROCESS

"We understand that the **Security Rule does not prescribe a specific risk analysis methodology,** recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization. Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve."

Clearwater

Risk Framing Strategy

Organizations should consider having a forma risk framing strategy. (See NIST SP 800-39)

Element	Description
Risk Assumptions and Constraints	This includes assumptions that affect how risk is conceptualized and constraints that limit organizational choices regarding risk responses.
Risk Tolerance	Defines the level of risk that an organization is willing to accept. This helps to guide decision-making when evaluating whether to mitigate, transfer, accept, or avoid specific risks.
Priorities and Trade-offs	Identifies organizational priorities that influence risk decisions and acknowledges that trade-offs will be necessary to manage risk effectively within the constraints of operational efficiency, cost, and mission objectives.
Roles and Responsibilities	Clearly delineates the roles and responsibilities within the organization for managing risk. This ensures accountability and establishes who has the authority to make risk-based decisions.
Risk Management Strategy	Articulates how the organization plans to address risk, including methods for risk assessment, risk response strategies, and how risk activities will be integrated into the broader organizational processes.
Stakeholder Engagement and Communication	Outlines how stakeholders will be involved in the risk management process and how information about risks and risk management activities will be communicated across the organization and to external stakeholders as appropriate.

Risk Analysis Related Audit Criteria

The audit criteria related to risk analysis evaluates policies and procedures as well as the risk analysis itself.

Policies and Procedures

1. Obtain and review risk analysis policies and procedures.
2. Evaluate and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated.

Risk Analysis

1. Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI has been conducted.
2. Evaluate and determine if the risk analysis documentation contains:
   a) A defined scope that identifies all of its systems that create, receive, maintain, or transmit ePHI.
   b) Details of identified threats and vulnerabilities.
   c) Assessment of current security measures.
   d) Impact and likelihood analysis.
   e) Risk rating.

Summing Up

Required

Risk analysis is required under the HIPAA Security Rule for all Covered Entities and Business Associates.

Comprehensive

The risk analysis needs to be comprehensive in scope covering all systems and associated components used to create, receive, maintain or transmit ePHI.

Aligned

The Risk Analysis should align with OCR's Guidance Risk Analysis Requirements Under the HIPAA Security Rule.

Ongoing

Risk Analysis should be ongoing or continuous in nature. Organizational, personnel, technology, facility, and threat changes along with a recent breach are all reasons to conduct risk analysis.

Additional Resources

On-demand Webinars

- Understanding OCR-Quality Risk Analysis: A Discussion with Former OCR Director Roger Severino
- From Risk Analysis to Risk Reduction: A Step-by-Step Approach
- Cybersecurity Fundamentals: Keys to an Effective Security Risk Analysis

Blogs and Whitepapers

- Critical Differences Between HIPAA Security Evaluations and Risk Analysis
- Risky Business: How to Conduct a NIST-based Risk Analysis to Comply with the HIPAA Security Rule
- Let the Buyer Beware: The Need for HIPAA Risk Analysis in Healthcare M&A Transactions
- Industry at Risk: Reconsidering the One-Size-Fits-All Approach to Healthcare Risk Analysis
- Why Your Point-in-Time Risk Analysis Isn't Enough
- Tips to Effectively Fund Your Enterprise Cyber Risk Management Program (ECRM)

Q&A

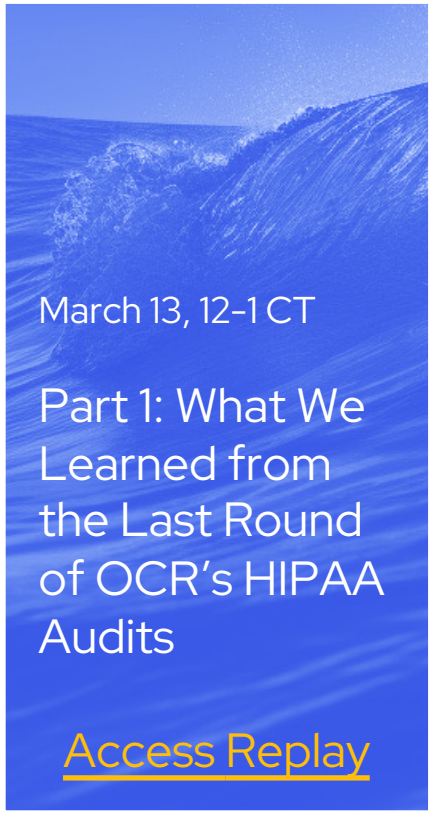
Jon Moore

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

OCR's HIPAA Audits On the Way – Clearwater Education

Register to attend Clearwater's 5 Part Series to Prepare for Anticipated Audits



March 13, 12-1 CT

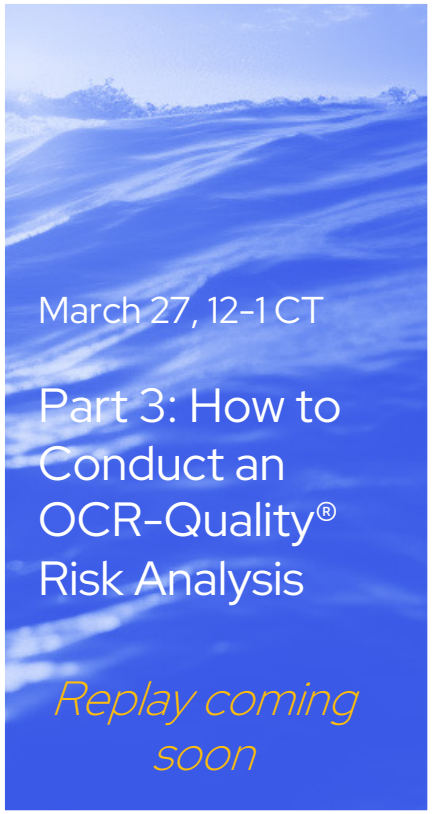
Part 1: What We Learned from the Last Round of OCR's HIPAA Audits

Access Replay

March 20, 12-1 CT

Part 2: Keys to Implementing an OCR-Quality® Compliance Program

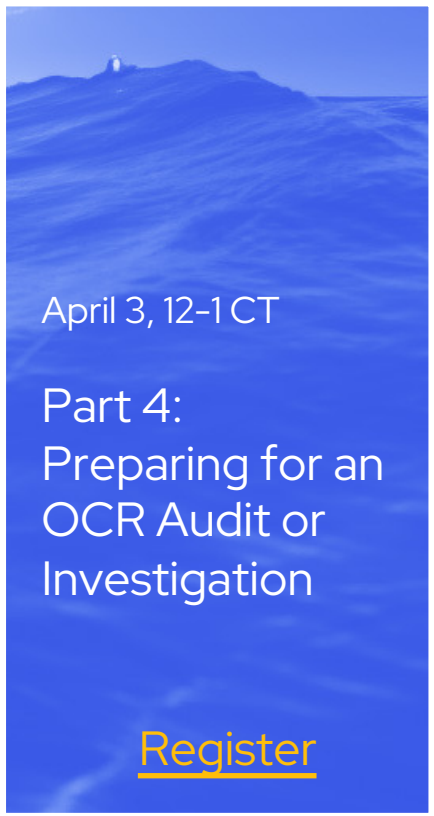
Access Replay



March 27, 12-1 CT

Part 3: How to Conduct an OCR-Quality® Risk Analysis

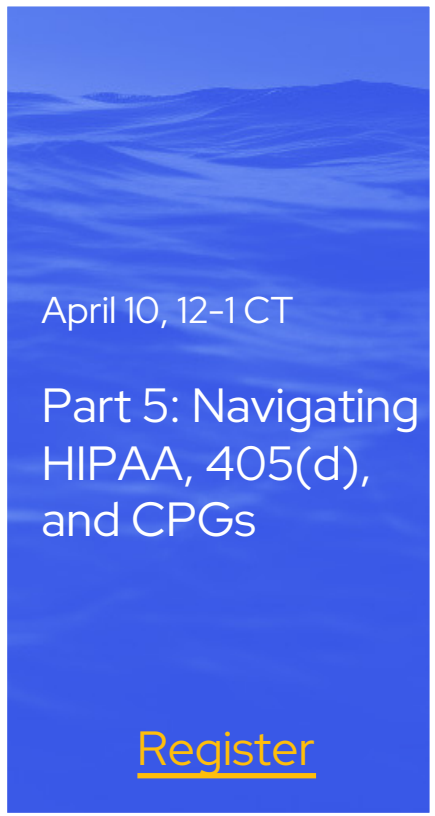
Replay coming soon



April 3, 12-1 CT

Part 4: Preparing for an OCR Audit or Investigation

Register



April 10, 12-1 CT

Part 5: Navigating HIPAA, 405(d), and CPGs

Register

Clearwater

Upcoming Events

April Cyber Briefing | April 4th

MWE Digital Health Forum | April 10 – 11, 2024

- Clearwater sponsoring

HCCA Annual Compliance Institute | April 14 – 17, 2024

- Dawn Morgenstern & Andrew Mahler speaking
- Booth #300

TN HIMSS Summit24 | April 18, 2024

- Clearwater sponsoring
- Leading a cybersecurity panel discussion

Clearwater

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Twitter | @clearwaterhipaa

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.