Secure and Compliant: OCR-Quality® Risk Management in Action

Webinar: Wednesday, October 1 @ 12:00 CT

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Agenda + Speakers

- Introductions
- Educational Content: Secure & Compliant: OCR-Quality Risk Management in Action
- Q+A

Steve Cagle, MBA, HCISPP, CHISL, CDH-E

Board Advisor
Clearwater

Lori Dutcher

Chief Compliance Officer
Beth Israel Lahey

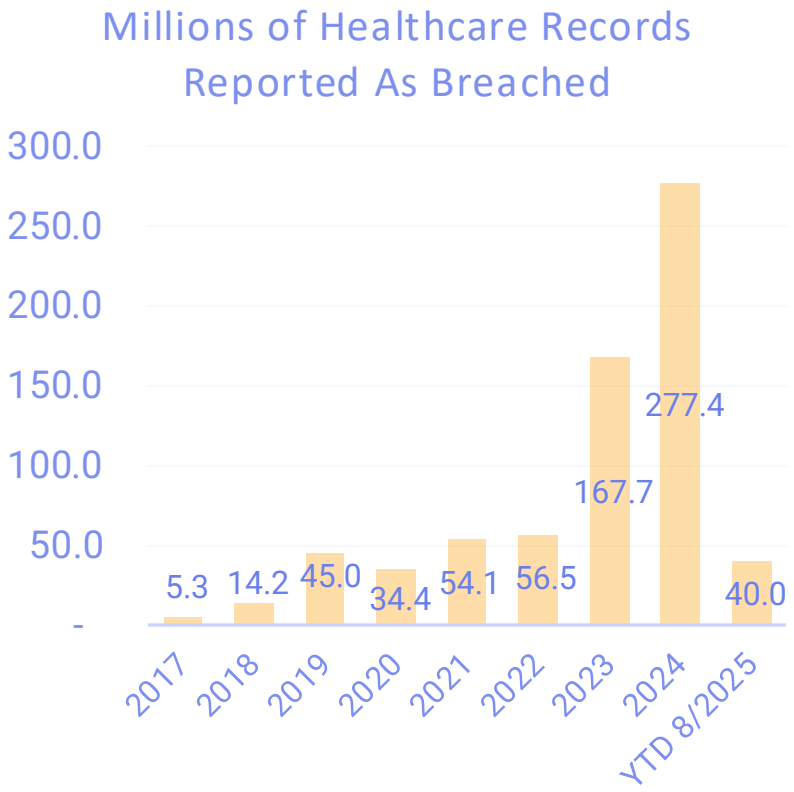
Dave Bailey, EMBA, CISSP

VP, Consulting Services, Security
Clearwater

Clearwater

Threats to Healthcare Continue to Grow

Breaches in healthcare continue to break records, and ransomware attacks are increasing, are more damaging and are taking longer to recover from.



Healthcare organizations report a ransomware attack last 12 months

2023	2024
60%	67%

> than 1 week to recover

2023	2024
50%	79%

Why are cyber attacks increasing in healthcare and becoming harder to recover from?

- Growing attack surface with more vulnerabilities
- ePHI is most valuable data
- Most likely to pay ransom
- Number of attackers increasing
- TTPs are evolving quickly
- Weak security programs
- Limited resources

1 The HHS Breach Portal (2024 data through 12/31/24, pulled on 1/31/25; 2023 data pulled 11/3/24) + 90 million additional records Change Healthcare announced earlier this year
2 The State of Ransomware in Healthcare 2024 – Sophos News

Clearwater

OCR Risk Analysis Enforcement Initiative

In October 2024, HHS Office for Civil Rights (OCR) launched its "Risk Analysis Initiative," focusing on enforcing the HIPAA Security Rule's risk analysis requirement.

Risk Analysis Requirement

"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 [organization]. Section 164.308(a)(1)(ii)(A).

10

Enforcement actions under Initiative announced since its introduction last fall

Key quotes from new OCR Director Paula Stannard:

"A HIPAA risk analysis is essential for identifying where ePHI is stored and what security measures are needed to protect it."

"Conducting a thorough HIPAA-compliant risk analysis (and developing and implementing risk management measures to address any identified risks and vulnerabilities) is even more necessary as sophisticated cyberattacks increase."

"Completing an accurate and thorough risk analysis that informs a risk management plan is a foundational step to mitigate or prevent cyberattacks and breaches."

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 at 45 CFR § 164.308(a)(1)(ii)(A).

93%

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.

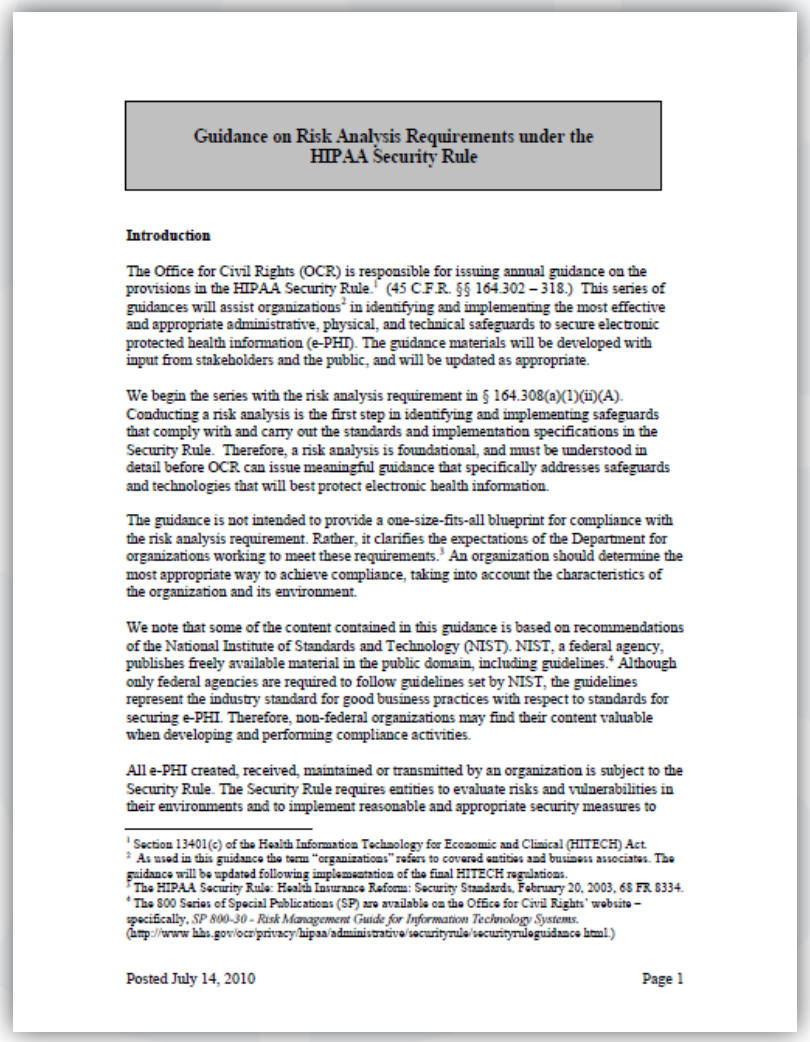
17%

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

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

A Risk Analysis Should Meet All 9 Elements of OCR's Guidance

1. Ensure Comprehensive Scope of the Analysis – All systems with ePHI
2. Document Information Asset Inventory
3. Identify and Document Potential Threats and Vulnerabilities (Risks)
4. Assess Current Security Measures (Controls)
5. Determine the Likelihood of Threat Occurrence
6. Determine the Potential Impact of Threat Occurrence
7. Determine the Level of Risk (Likelihood x Impact)
8. Finalize Documentation
9. **Periodic Review and Updates to the Risk Assessment**
10. Meet Emerging OCR Standard of Care (raising the bar)



Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Introduction

The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.[1] (45 C.F.R. §§ 164.302 – 318.) This series of guidances will assist organizations[2] in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate.

We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A). Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements.[3] An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.

We note that some of the content contained in this guidance is based on recommendations of the National Institute of Standards and Technology (NIST). NIST, a federal agency, publishes freely available material in the public domain, including guidelines.[4] Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.

All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to

[1] Section 13401(c) of the Health Information Technology for Economic and Clinical (HITECH) Act.
[2] As used in this guidance the term "organizations" refers to covered entities and business associates. The guidance will be updated following implementation of the final HITECH regulations.
[3] The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.
[4] The 800 Series of Special Publications (SP) are available on the Office for Civil Rights' website – specifically, *SP 800-30 - Risk Management Guide for Information Technology Systems.* (http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.)

Posted July 14, 2010 Page 1

[OCR Risk Analysis Guidance]
[NIST SP 800-30 Guide for Conducting Risk Analysis]

Clearwater

Risk Analysis v. Gap Assessment

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, NIST SP 800-171, 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 and standards: HIPAA Security Rule, GDPR, PCI, HITRUST

Link to Differences Between HIPAA Security Evaluations and Risk Analysis - Clearwater

Clearwater

Typical Causes of Insufficient Risk Management Program

There are several reasons risk management programs fail both in the Analysis Phase as well as the Response Phase.

Lack ePHI System Inventory	Risk assessments are not granular enough	Risks are not responded to or updated	Inability to effectively report to Governing Body
Organizations don't know where their ePHI and other sensitive data lives and goes and therefore cannot assess all security risks.	High level assessments don't tell the organization anything new, or where specific issues are. They are quickly out of date. Gaps are missed.	Security teams struggle to create risk mitigation action plans, drive them forward, and keep them up to date because they lack people and tools.	Security programs are underfunded, and resource constrained, because CISOs can't communicate risks or ROI on their program.

Q&A

Upcoming Webinars

Speaking the Same Language: Building Trust Between Security and the Enterprise | Monthly Cyber Briefing | October 9

- The latest intelligence on threat actors and regulatory developments impacting healthcare and a Fireside chat with Clearwater's CEO, Steve Cagle and Tracy Touma, Cybersecurity Business Liaison, Cleveland Clinic
- Register Here

HIPAA Compliance: It's a Time for a Remodel – 2025 Update | October 16

- Join Clearwater Senior Director of Consulting Services Dawn Morgenstern as she breaks down the latest regulatory changes and shares actionable strategies to help you modernize compliance efforts
- Register Here

Upcoming Events

Hospital Horizons Symposium 2025 | October 6–7, 2025 | Washington, DC

- Clearwater is proud to sponsor the second annual **Hospital Horizons Symposium**, hosted by Holland & Knight.
- Andrew Mahler speaking on an Innovation Panel on Oct 7th.
- Register & learn more here

SCALE Healthcare Leadership Conference | October 14, 2025 | New York, NY

- Clearwater is a proud sponsor
- Clearwater leading a panel discussion "Cyber Risk and the Threat to MSO Value Creation"
- Learn more & register here

- Look for the Clearwater team in the Digital Health Hub Foundation / StartUp Health Pavilion
- Learn more here

Clearwater

We are here to help.

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

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

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

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.