Keys to Implementing an OCR-Quality® Compliance Program

Dawn Morgenstern | MBA, CHPC, CCSFP

Wes Morris | CHPS, CIPM, HCISPP

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

- Introduction
- How the Rules Developed
- Related Rules
- Survey of Technology in use when the HIPAA Rules Were Promulgated
- Using the Audit Protocols to Improve Compliance Programs
- Sources of Guidance in addition to the Rules
- Ten Key Elements to ensuring OCR-Quality Compliance Programs
- Conclusion

About Your Presenters

Dawn Morgenstern, MBA, CHPC, CCSFP

Senior Director, Consulting Services, Privacy & Compliance

- 20 years diverse experience in complex health care systems, including hospitals, clinics, pharmacies, specialty pharmacy programs, pharmacy mail order, respiratory and infusion therapy and home medical equipment, and pharmacy benefit management
- 15 years as privacy program leader, with ability to prioritize, design, resource, and implement complex enterprise-wide compliance solutions
- Direct coordination with investigative bodies (e.g., Office for Civil Rights, FTC) and other legal entities relating to compliance reviews and complaint investigations
- Former corporate Privacy Official & Financial Privacy Officer for large health care organization consisting of 8,000+ retail and clinic/health center locations
- Former privacy advisory positions with the Confidentiality Coalition and National Association of Chain Drug Stores

LinkedIn - Dawn Morgenstern

About Your Presenters

Wes Morris, CHPS, CIPM, HCISPP

Senior Director, Consulting Services

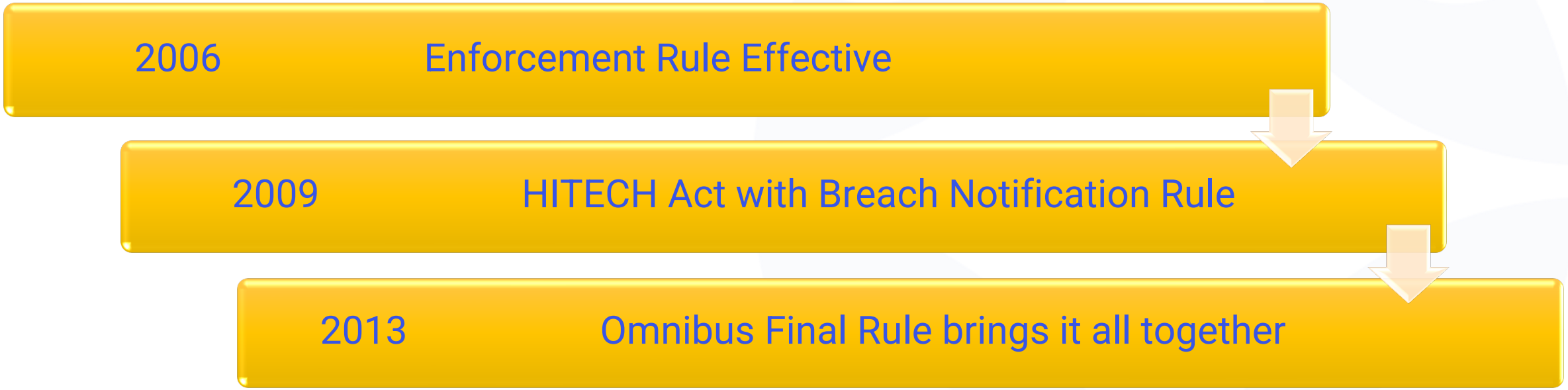
- 20 years in Clinical Care/Social Services, with emphasis in management of organizations under 42 CFR Part 2 (Confidentiality of Substance Use Disorder records and patients)
- 20 years in HIPAA Privacy and Security as Privacy Officer, Security Officer and Subject Matter Expert in large systems and governmental agencies
- 10 years with Clearwater providing consultation and management to hospitals, health systems and their supporting businesses
- American Health Information Management Association (AHIMA) Privacy and Security Practice Council (2019, 2022, 2023 Council Co-Chair)
- AHIMA Exam Development Committee for the Certified in Healthcare Privacy and Security (CHPS) credential (2013-2021)
- 2019 - 2021 Director of Legal/Legislative Affairs and Advocacy for the Idaho HIMA Board of Directors

LinkedIn - Wes Morris

Introduction

How the Rules Developed

How the Rules Developed (Continued)



Related Rules

2013	Genetic Information Nondiscrimination Act (GINA) 2009, Amended in HIPAA 2013
2014	Clinical Laboratory Improvement Amendments (CLIA) and HIPAA Privacy Rule
2015	Cybersecurity Act Section 405(d)
2020	21st Century Cures Act (Cures Act) Information Blocking final rule
2021	H.R. 7898 (Public Law 116-321) – Amended HITECH Act to require HHS to consider recognized security practices of CEs and BAs
2021	Notice of Proposed Rulemaking (NPRM) to the HIPAA Privacy Rule (not final)

More Related Rules

2023	NPRM – Cures Act: Establishment of Disincentives for HC Providers that have Committed Info Blocking (Not final)
2023	NPRM – HIPAA Privacy Rule to Support Reproductive Health Care Privacy (not final)
2024	Health Data, Technology, and Interoperability […] (HTI-1) Final Rule
2024	HIPAA Audit Review Survey Notice
2024	Confidentiality of Substance Use Disorder Patient Records Final Rule

About the HIPAA Audit Protocols

- An ”Open Book Test”
  - Expresses the evidence a CE or BA will have to show
  - OCR will evaluate samples that are spelled out in the Audit Inquiry column of the Audit Protocol

45 C.F.R.	Assigned Security Responsibility
§164.308(a)(2): Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Does the entity have **policies and procedures** in place regarding the establishment of a security official?
	Has the entity **identified the security official** responsible for the development and implementation of the policies and procedures required by this subpart?
	Obtain and review documentation of the assigned Security Official(s) responsibilities (e.g., job description) and that a ***natural person has been named*** to act as the Security Official and/or other individuals have been assigned with other security duties. Evaluate and determine whether...responsibilities of the Security Official have been clearly defined.

Perspective – Technology and Events 2003 - 2005

- Top Movies - Finding Nemo, Elf, Napoleon Dynamite
- Blu-ray optical disc is released, to replace DVD technology
- Myspace was founded –reached 100 million plus users before being overtaken by Facebook
- Google floats its publicly traded stock after solving how to profit from search
- Hacker group Anonymous forms, performing “hacktivism” against websites like the Motion Picture Association of America before moving on to governmental targets
- The “candy bar cell phone” was the top seller

Features

- 50 Contacts
- 50 Text Messages
- Flashlight
- Calculator
- Stopwatch

Clearwater

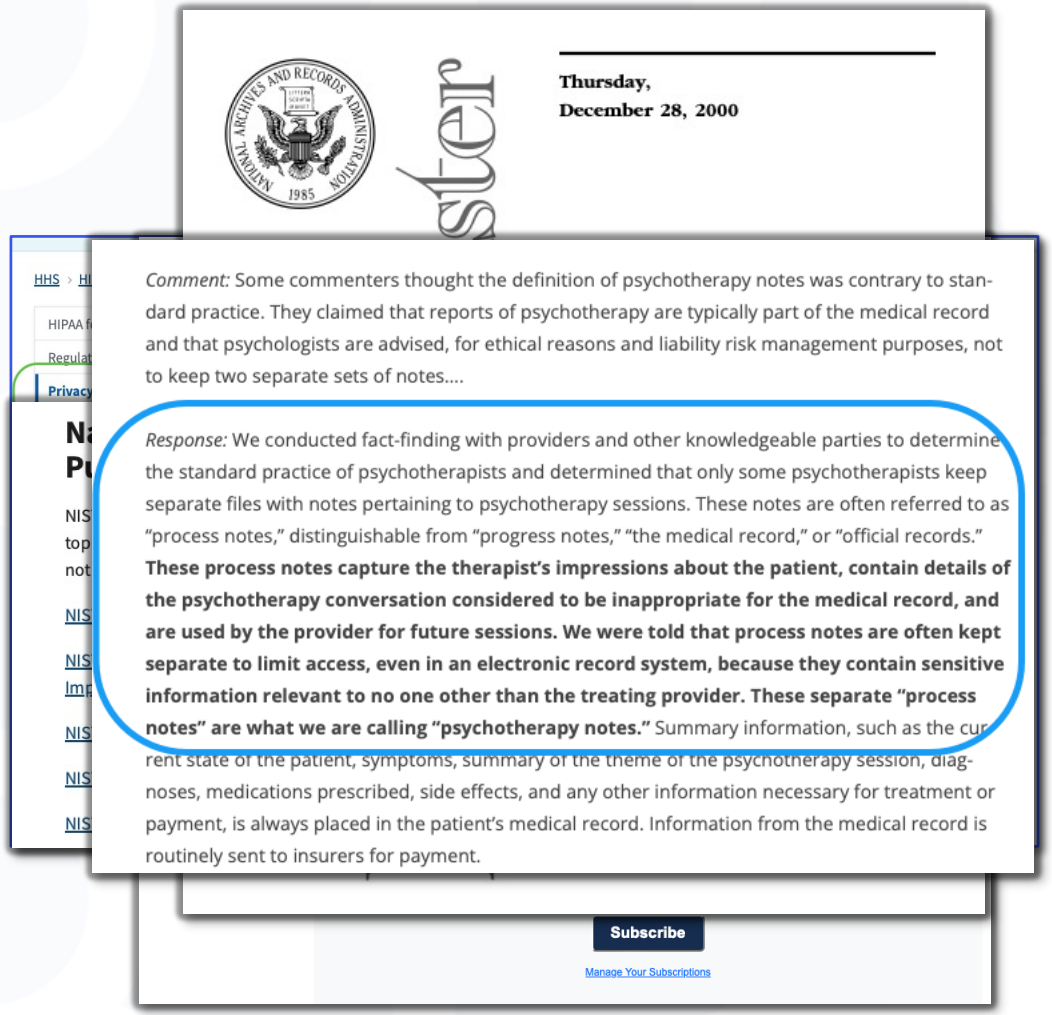
The Essential Question

If the rules have been around so long, why do we still struggle with effective implementation?

To *Fully* Understand Compliance Responsibilities

Go beyond the rules and the Audit Protocols

- The Preamble to each rule and Response to Comments on publication provide significant clarification of intent
  - Example – Psychotherapy Notes
- OCR provides guidance under HIPAA for Professionals
- Subscribe to the OCR Email Updates
- NIST Special Publications are essential to the HIPAA Security Rule



10 Key Areas of a HIPAA Compliance Program

1

Set privacy and security risk management & governance program in place

45 CFR § 164.308(a)(1)

2

Develop & implement privacy, security, & breach notification policies & procedures

45 CFR §§ 164.530 and 164.316

3

Train all members of your workforce

45 CFR §§ 164.530(b) and 164.308(a)(5)

4

Complete a HIPAA security risk analysis

45 CFR § 164.308(a)(1)(ii)(A)

5

Complete HIPAA security risk management

45 CFR § 164.308(a)(1)(ii)(B)

6

Complete a HIPAA security evaluation (e.g., "compliance assessment")

45 CFR § 164.308(a)(8)

7

Complete technical testing of your environment

45 CFR § 164.308(a)(8)

8

Implement a strong, proactive Business Associate management program

45 CFR §§ 164.502(e) and 164.308(b)

9

Privacy Rule and Breach Rule compliance assessments

45 CFR §§ 164.530 and 164.400

10

Document and act upon a remediation plan

45 CFR §§ 164.530(c) and 164.306 (a)

Derived from OCR Enforcement Actions. Demonstrate Reasonable Diligence.

Clearwater

Final Thoughts

Q&A

Wes Morris| Dawn Morgenstern

Resources

- 2023
  - HIPAA Privacy Rule To Support Reproductive Health Care Privacy – NPRM – April 17, 2023 (OCR)
  - Healthcare & Public Health Sector Coordinating Council – April 17, 2023
    - Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
    - Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations
    - Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations
    - Hospital Cyber Resiliency Initiative Landscape Analysis
  - Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing – HTI-1 – Proposed Rule – April 18, 2023 (ONC)
  - Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules – Final Rule – July 3, 2023 (OIG)
  - Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure – Final Rule – August 4, 2023 (SEC)
  - 21st Century Cures Act: Establishment of Disincentives for Health Care Providers – Proposed Rule – November 1, 2023 (CMS/ONC)

Resources

- 2024
  - Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing – HTI-1 – – Final Rule – January 9, 2024 (ONC)
  - Healthcare and Public Health (HPH) Cybersecurity Performance Goals – January 24, 2024
  - HIPAA Audit Review Survey – Notice – February 12, 2024 (HHS)
  - Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (NIST SP 800-66r2) – February 14, 2024 (NIST)
  - Confidentiality of Substance Use Disorder (SUD) Patient Records – Final Rule – February 16, 2024 (SAMHSA)
  - Annual Report to Congress on Breaches of Unsecured Protected Health Information – February 22, 2024 (HHS/OCR)
  - Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance – February 22, 2024 (HHS/OCR)
  - The NIST Cybersecurity Framework (CSF) 2.0 – February 26, 2024 (NIST)

Additional Links and Resources

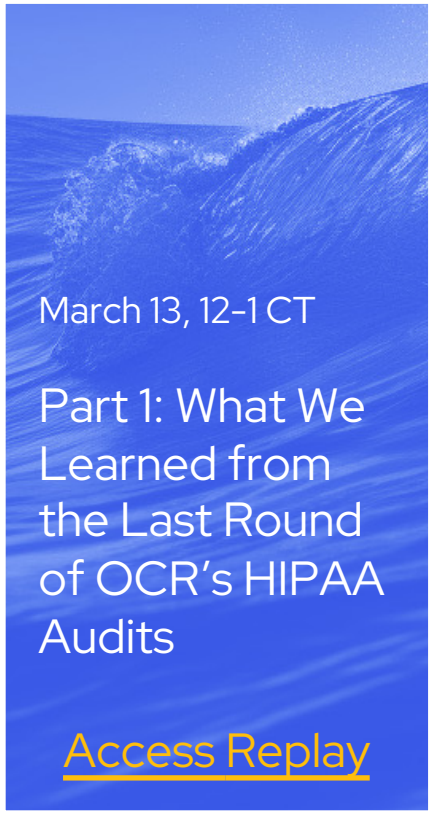
- HHS/OCR HIPAA Audit Protocol
- December 2000 Privacy Rule Publication that references Psychotherapy Notes and the Response to Commenters
- HHS/OCR HIPAA Guidance
- HHS/OCR Subscribe to email updates

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 Free Education

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



March 13, 12-1 CT

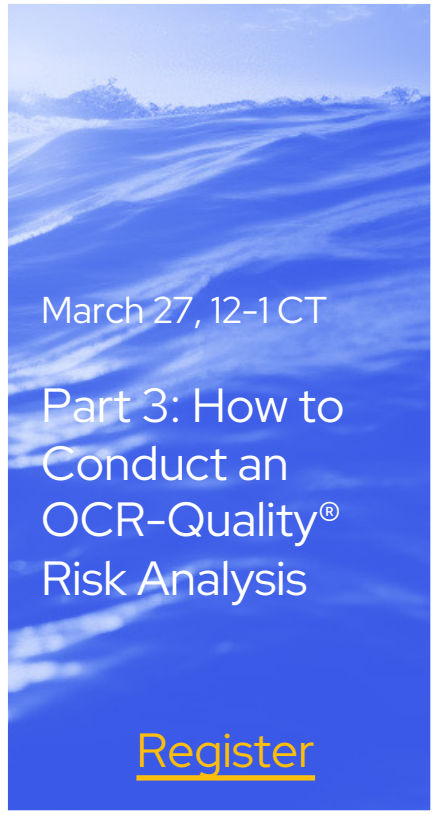
Part 1: What We Learned from the Last Round of OCR's HIPAA Audits

Access Replay

March 20, 12-1 CT

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

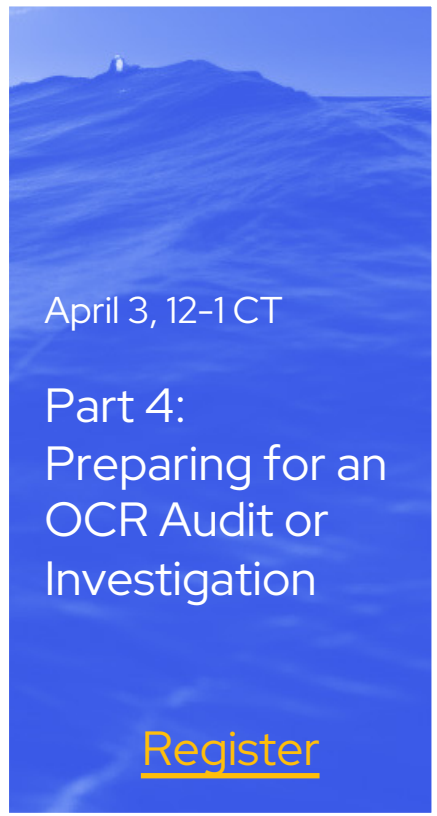
Replay coming soon



March 27, 12-1 CT

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

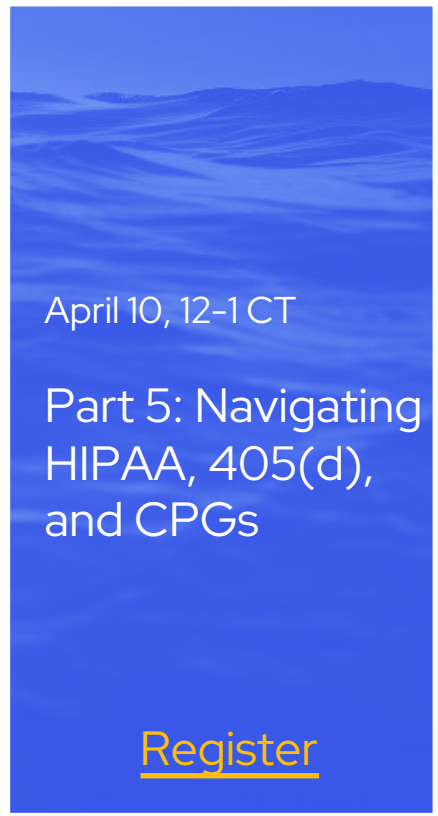
Register



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.