What We Learned From the Last Round of OCR's HIPAA Audits

Andrew Mahler, JD, CIPP/US, CHC, CHPC, CHRC
Omenka Nwachukwu, Esq.

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
- Summary
- Audit Results
  - Notice of Privacy Practices
  - Right of Access
  - Content of Breach Notification
  - Security Risk Analysis
  - Security Risk Management
- Conclusion

About Your Presenters

Andrew Mahler, JD, CIPP/US, CHC, CHPC, CHRC

Vice President, Consulting Services, Privacy & Compliance

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

- **Former OCR Investigator**
  - Led enforcement actions and investigations as a former Investigator for the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), ensuring compliance with health information privacy and civil rights regulations.
- **Seasoned Privacy Officer**
  - Served as Chief Privacy Officer/Enterprise Privacy Officer for academic medical centers and related health systems, bringing over a decade of experience in privacy, compliance, and research compliance leadership roles.
- **Legal Expertise and Certifications**
  - Holds various certifications including CIPP/US, CHC, CHPC, and CHRC, coupled with licensure to practice law in Georgia and Arizona, offering a comprehensive understanding of healthcare law, HIPAA compliance, and data privacy.
- **Educational and Publishing Contributions**
  - Developed healthcare law courses, acted as an expert witness in HIPAA and data privacy cases, and actively publishes and presents on pertinent topics, demonstrating a commitment to advancing knowledge in the field of OCR compliance.

About Your Presenters

Omenka Nwachukwu, Esq.

Privacy Consultant

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

- **Former OCR Investigator**
  - Possesses over 2 years as a HIPAA Privacy Investigator for the Office for Civil Rights, U.S. Department of Health and Human Services, specializing in complex complaints related to Right of Access and PACS server insecurity violations.
- **Expertise in HIPAA Compliance**
  - Demonstrates comprehensive knowledge of the Health Insurance Portability and Accountability Act (HIPAA) and its application to covered entities, enabling thorough assessment of complaints for "high-impact" issues and potential civil money penalties.
- **Investigative Skills**
  - Developed and drafted investigative plans, data requests, and witness interview questions, showcasing the ability to effectively navigate investigations and gather crucial information.
- **Legal Background and Representation**
  - Brings over 3 years of experience in workers' compensation insurance defense, representing clients of various sizes in mediations, depositions, and court proceedings, ensuring robust legal representation and resolution of cases

Introduction

Why Are We Here?

- Section 13411 of HITECH requires HHS to audit covered entity and business associate compliance with the HIPAA Rules:
  - "The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this Act, comply with such requirements."
- OIG Reports:
  - *OCR Should Strengthen Its Oversight of Covered Entities' Compliance With the HIPAA Privacy Standards*
  - *OCR Should Strengthen Its Follow up of Breaches of Patient Health Information Reported by Covered Entities*
- Phase I Audits (2011-2012) and Phase II Audits (2016-2017)

Phase 1 and Phase 2 Audits

- *Phase 1*: In 2011 and 2012, OCR implemented a pilot audit program, auditing 115 covered entities.
  - Included on-site visits
- *Phase 2*: From 2016 to 2017, OCR audited 166 covered entities and 41 business associates.
  - Desk audits
- On December 17, 2020, the Office for Civil Rights (OCR) issued its 2016-2017 HIPAA Audits Industry Report. The Industry Report provides:
  - A snapshot of HIPAA compliance within a sample of the healthcare industry, based on the OCR Audit Protocol.
  - Examples of widespread noncompliance.
  - Recommendations from OCR and opportunities for improvement.

2024 Notice of Proposed Rulemaking

- Federal Register / Vol. 89, No. 29 / Monday, February 12, 2024
- "This information collection consists of 39 online survey questions that will be sent to 207 covered entities and business associates that participated in the 2016–2017 OCR HIPAA Audits. The survey will gather information relating to the effect of the audits on the audited entities and the entities' opinions about the audit process..."
- "The information, opinions, and comments collected using the online survey will be used to improve future OCR HIPAA Audits."

"OCR intends to initiate audits of HIPAA-regulated entities later this year. These audits can assist regulated entities in improving their HIPAA compliance and their protection of health information."

OCR Director, Melanie Fontes Rainer

February 14, 2024

What is OCR's Audit Process?

1. Identify covered entities over a wide range of health care providers, health plans, and health care clearinghouses.
   - Criteria: size, affiliations, location, and whether an entity was public or private.
   - Health plans divided into group plans and issuers.
   - Providers categorized by type of hospital, practitioner, elder care/skilled nursing facility (SNF), health system, or pharmacy.
2. Randomized selection of organizations in each category, and then selection of those organizations' business associates.

What is the OCR Audit Process? (cont.)

3. Two email communications: an initial notification letter and a document request.
4. 10 business days to respond to the document requests.
5. OCR reviews requested documentation against the audit protocol.
6. OCR provided draft findings and gave entities an opportunity to respond.
7. OCR considered an entity's responses when preparing the entity's final report.

Compliance Effort Rating – Phase 2 Audits

OCR rated compliance efforts for every audited element on a scale of 1 to 5.

Audit Compliance Effort Ratings - Legend	
Rating	Description
1	The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.
2	The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.
3	The audit results indicate the entity's efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.
4	Audit results indicate the entity made negligible efforts to comply with the audited requirements – e.g., policies and procedures submitted for review are copied directly from an association template' evidence of training is poorly documented and generic.
5	The entity did not provide OCR with evidence of a serious attempt to comply with the Rules.

Clearwater

Summary of 2016-2017 Audit Results

Protocol elements assessed in the 2016-2017 OCR Audit

Starred elements had results of widespread compliance failure.

HIPAA RULE	PROVISIONS EXAMINED IN COVERED ENTITY AUDIT	
Privacy Rule	Notice of Privacy Practices & Content Requirements §§ 164.520(a)(1) & (b)(1)	★
	Provision of Notice – Electronic Notice (Website Posting) § 164.520 (c)(3)(i)	
	Right of Access §§ 164.524(a)(1), (b)(1), (b)(2), (c)(2),(c)(3), (c)(4),(d)(1),(d)(3)	★
Breach Notification Rule	Timelines of Notification § 164.404(b)	
	Content of Notification § 164.404(c)(1)	★
Security Rule	Security Management Process – Risk Analysis § 164.308(a)(1)(ii)(A)	★
	Security Management Process – Risk Management § 164.308(a)(1)(ii)(B)	★

What did OCR find?

- Most covered entities failed to:
  - Provide all required content for a Notice of Privacy Practices.
  - Properly implement individual right of access requirements (e.g., respond within 30 days; reasonable cost-based fee).
  - Provide all required content for breach notification to individuals.
- Most covered entities and business associates failed to:
  - Implement the HIPAA Security Rule requirements for risk analysis and risk management.

Audit Results by Audited Element

Notice of Privacy Practices

45 C.F.R. §§ 164.520(a)(1) & (b)(1)

45 C.F.R. §§ 164.520(a)(1) & (b)(1)

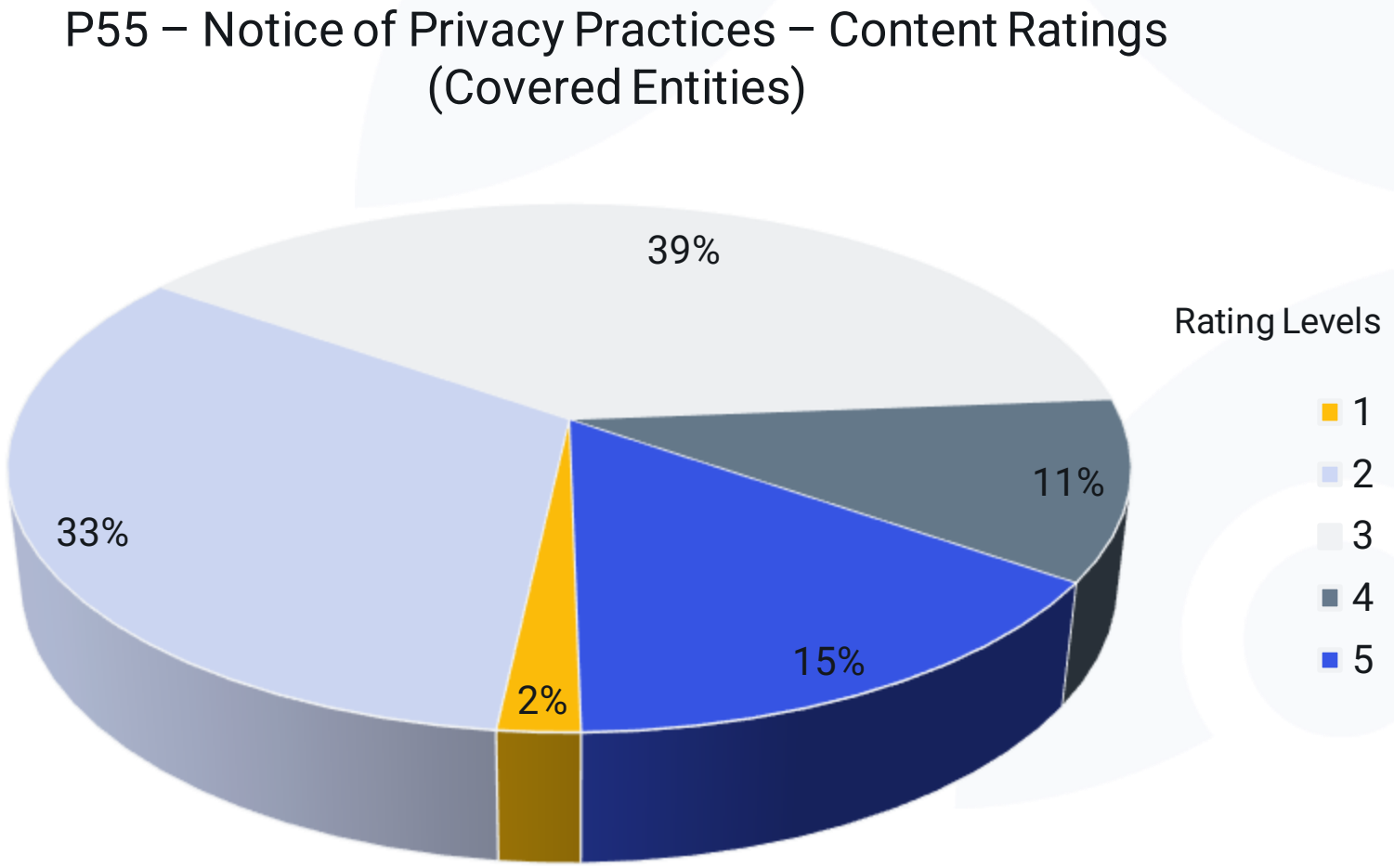
"An individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to PHI."

Notice of Privacy Practices

- **Documents Requested:**
  - Copy of NPP distributed to individuals.
  - Copy of all NPPs posted on entity website and within the facility.
- **Audit Results:**
  - 2/3 of covered entities failed to meet content requirements.
- **Recommendation:**
  - Use the Model Notices of Privacy Practices available on OCR's website.
    - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html
  - Utilize OCR's Audit Protocol.

Notice of Privacy Practices – Content Ratings

- 2/3 of covered entities failed to comply or made minimal/negligible efforts to comply.



Clearwater

Right of Access

45 C.F.R. §§ 164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)

45 C.F.R. §§ 164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)

"An individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set."

Right of Access

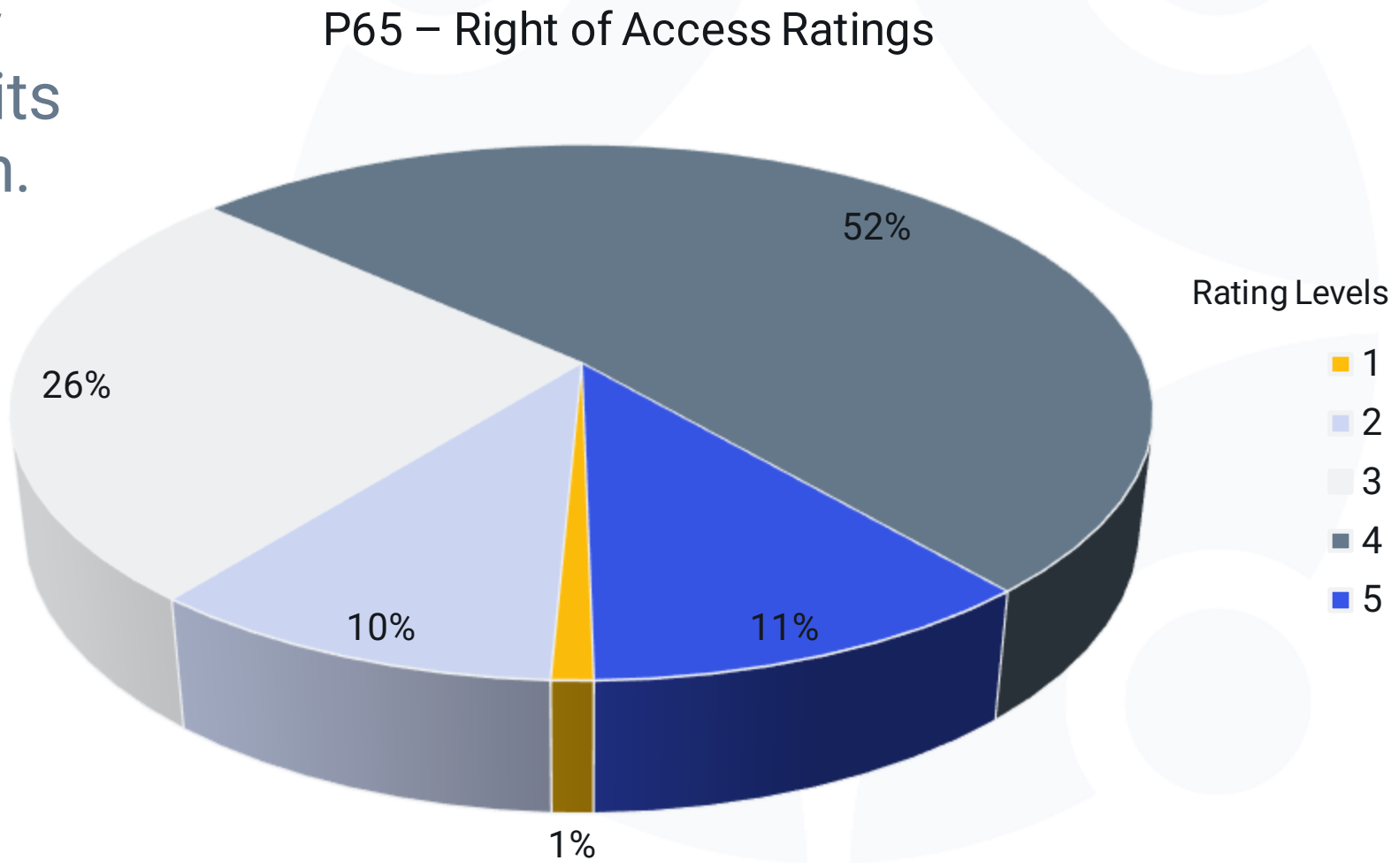
- **Documents Requested:**
  - Access requests.
  - Extensions to access requests.
  - Access requests templates and/or forms.
  - Notice of Privacy Practices.
  - Access policies and procedures.
- **Audit Results:**
  - Almost all covered entities audited (89%) failed to show they were correctly implementing the individual right of access.

Right of Access – Audit Results

- Recurring Issues:
  - Not documenting access requests.
  - Unreasonable cost-based fee policy or incorrect blanket fees.
  - Lack of policies regarding:
    - Requesting/accessing PHI or procedures for providing access.
    - Access to PHI not maintained by the entity.
    - Timely written denial and the basis for denying an access request.
  - Incorrectly denying access to:
    - PHI in a designated record set (e.g., test results, Rx history).
    - A designated third party.
    - PHI in the desired form/format (e.g., requiring in-office pick up).
  - Requiring individuals to submit signed authorization forms.
  - Notice of Privacy Practices did not:
    - Correctly describe individual rights.
    - Identify (or correctly identify) the patient's right to timely access.

Right of Access Ratings

- Only one audited entity received a 1 rating for its access implementation.



Clearwater

Right of Access - Recommendations

- Office of the National Coordinator for Health Information Technology (ONC)'s *Improving the Health Records Request Process for Patients*.
- Utilize OCR Audit Protocol questions to understand OCR's expectations for compliance.
- 2016-2017 HIPAA Audits Industry Report Appendix.

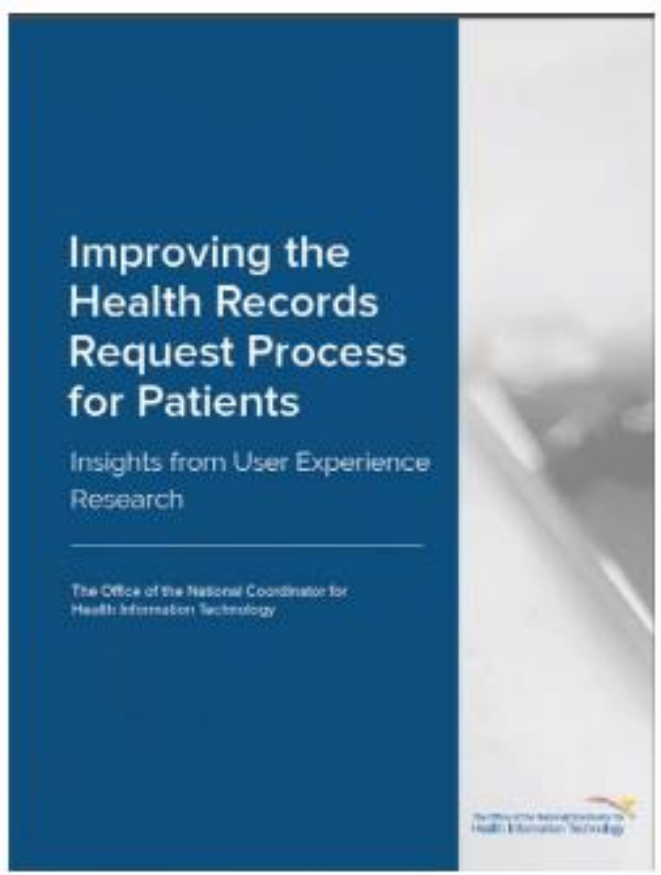


FIGURE 14 IMPROVING THE HEALTH RECORDS REQUEST PROCESS FOR PATIENTS

Clearwater

Content of Breach Notification

45 C.F.R. § 164.404(c)(1)

[Required elements of breach notification to affected individuals]

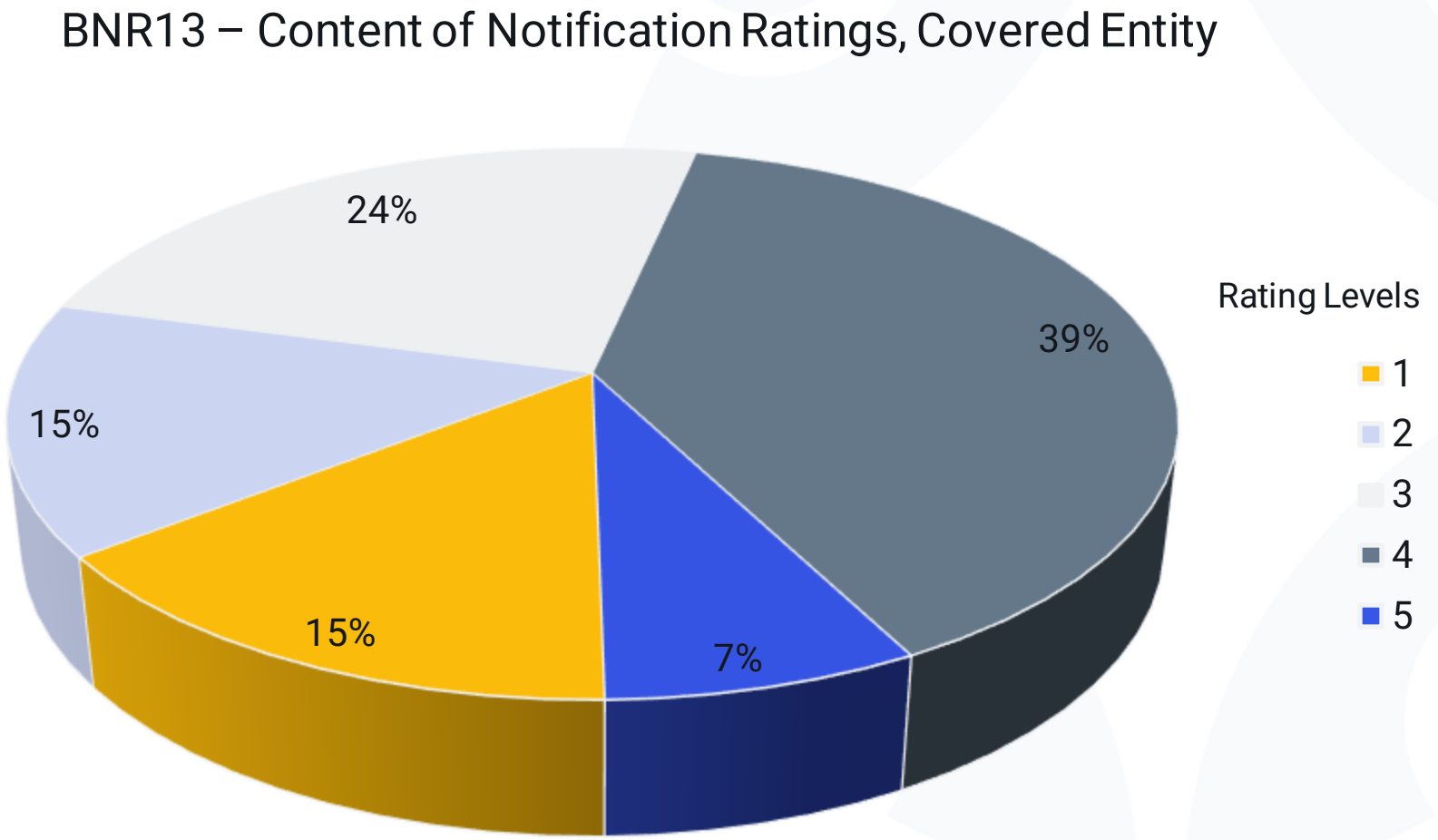
Content of Breach Notification

- **Documents Requested:**
  - Standard template or form letter for breach notification to individuals.
  - A list of breaches, if any, which occurred in the previous calendar year.
  - Written notice sent to affected individuals in the previous calendar year.
- **Audit Results:**
  - Most breach notification letters missing pieces of required content.
- **Recommendation:**
  - Train workforce members on:
    - Requirements for breach notification letters.
    - How to properly document and inform affected individuals.
    - De-identification.

Content of Breach Notification – Audit Results

- Frequently omitted content requirements:
  - Describe the unsecured PHI involved in the breach.
  - Steps for individuals to protect against potential harm from the breach.
  - Detailed explanation of the entity's investigation and mitigation activities.
  - No dates on the notification letters and documentation.
  - Inadequate contact information.
    - No way to ask questions or learn more information (e.g., toll-free telephone number, email, website, or postal address).

Content of Notification Ratings, Covered Entity



Clearwater

Security Risk Analysis

45 C.F.R. § 164.308(a)(1)(ii)(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.

Security Risk Analysis

- **Requested Documents:**
  - Current and prior risk analyses and results.
  - Risk analysis policy and procedures.
  - Documentation of risk analysis process and evidence the documentation is periodically reviewed and updated.
- **Audit Results:**
  - Few covered entities (14%) and business associates (17%) conduct risk analysis activities.

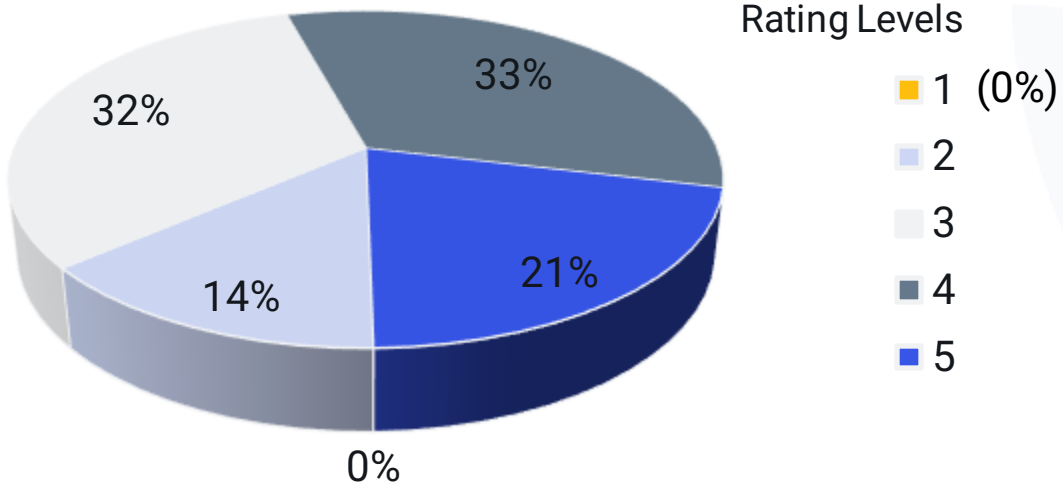
Security Risk Analysis – Audit Results

- Entities failed to:
  - Identify and assess the risks to all their ePHI.
  - Develop and implement policies and procedures re: risk analysis.
  - Identify threats/vulnerabilities, consider potential likelihoods and impacts, and rate the risk to ePHI.
  - Review and update a risk analysis after:
    - Changes in the environment and/or operations.
    - Security incidents.
    - A significant event.
  - Conduct risk analyses consistent with policies and procedures.

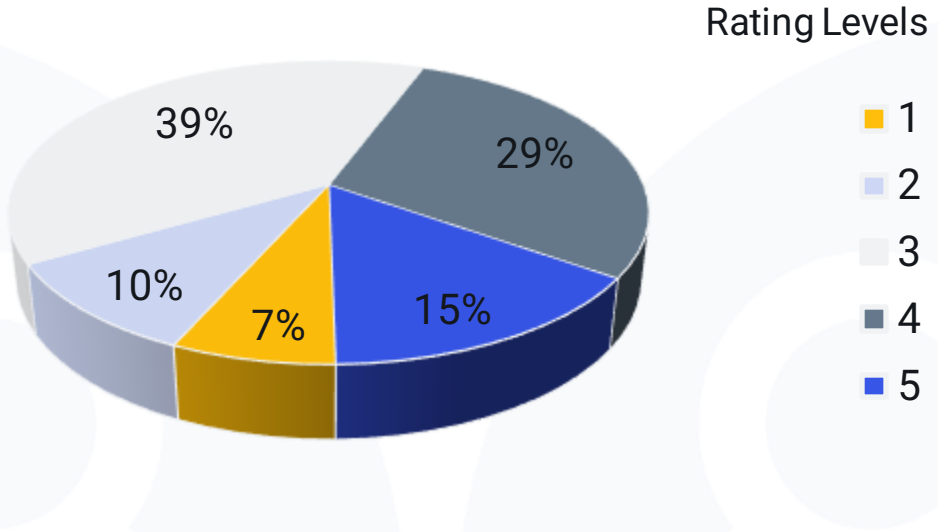
Risk Analysis Ratings

- Business associates generally showed greater compliance than covered entities

S2 – Risk Analysis Ratings – **Covered Entities**



S2 – Risk Analysis Ratings – **Business Associate**



Clearwater

Security Risk Analysis - Recommendations

- The responsibility to conduct appropriate risk analyses rests with the entity.
  - Many entities rely on third parties to manage or perform risk analyses. However, these third parties frequently failed to meet the requirements.
  - Entities incorrectly assumed that a purchased security product satisfied all Security Rule requirements.
- Entities must understand and comply with risk analysis requirements to appropriately safeguard PHI.
- Guidance to include risk analysis in risk management programs:
  - Technical assistance from OCR, ONC and the National Institute of Standards and Technology (NIST).

Security Risk Management

45 C.F.R. § 164.308(a)(1)(ii)(B)

Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Security Risk Management

- **Documents Requested:**
  - Documentation of efforts used to manage risks.
  - Risk management policies and procedures.
  - Evidence that current and ongoing risks are reviewed and updated.
  - Evidence that the risk management process is reviewed and updated.
- **Audit Results:**
  - 94% of covered entities and 88% of business associates failed to implement appropriate risk management.
  - Some identified risks but failed to implement appropriate security measures.

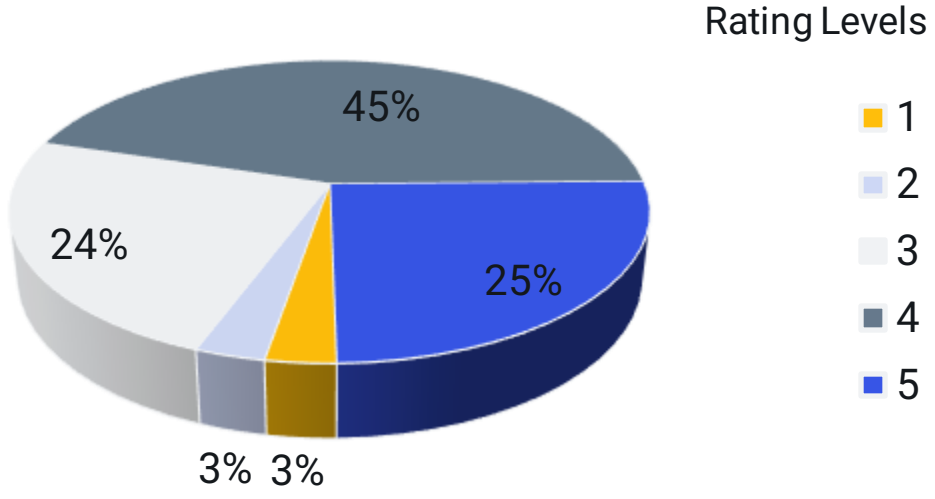
Security Risk Management – Audit Results

- Lacking technical safeguards (access controls, audit controls, etc.) needed to protect ePHI.
- Not knowing:
  - Acceptable levels of risk.
  - Vulnerabilities applicable to their environment.
  - How to mitigate risks or vulnerabilities to ePHI in their organization.
- Assessing potential risks and vulnerabilities to some ePHI instead of all.
- No remediation plans, or not implementing within a reasonable timeframe.
- Implementing a risk management plan but failing to update it.

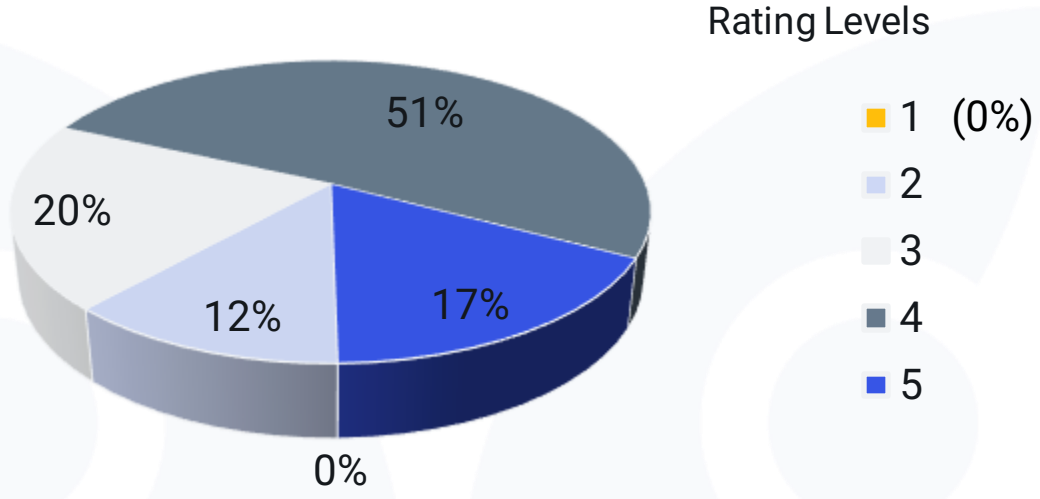
Security Risk Management Ratings

- Business associates generally showed greater compliance than covered entities.

S3 – Risk Management Ratings – **Covered Entities**



S3 – Risk Management Ratings – **Business Associate**



Clearwater

Security Risk Management – Results and Recommendations

- Entities failed to:
  - Produce policies and procedures, or implement security measures, sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
- Reliance on contracted security firms does not remove the responsibility to establish a compliant security program.
- Entities can find resources for implementing appropriate risk management programs in the Appendix.

Conclusion

Summary and Final Thoughts

- Confirm the internal process/escalation and practice!
- NPPs are often missing elements—the HHS model NPP may help covered entities avoid this mistake.
- Inconsistent provision of access to PHI can improve with better procedures and digital technology using HHS technical assistance.
- Covered entities and business associates failed to implement effective risk analysis and risk management activities.
- Review your organization's risk analysis process.
  - Review OCR's Guidance on Risk Analysis Requirements.
- Review OCR's Annual Reports to Congress.
- Consider consulting with a third party to provide an independent review or mock audit/investigation.

Q&A

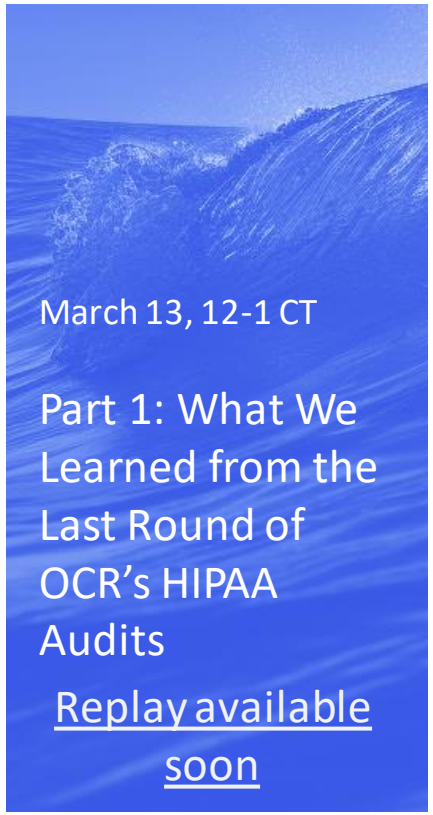
Andrew Mahler | Omenka Nwachukwu

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

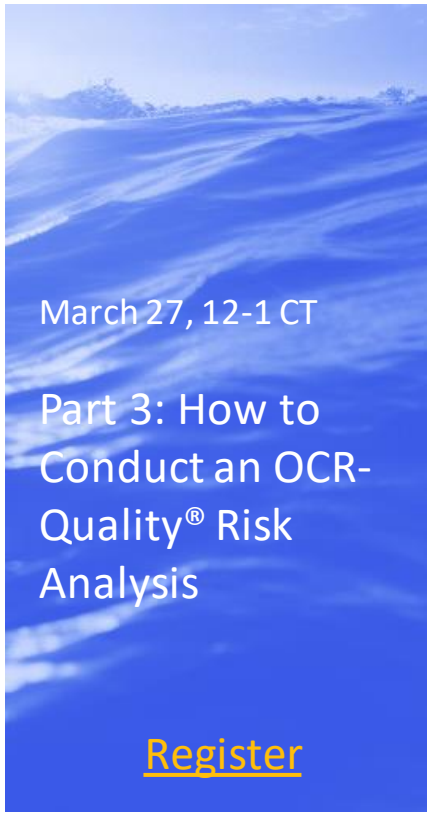
Part 1: What We Learned from the Last Round of OCR's HIPAA Audits

Replay available soon

March 20, 12-1 CT

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

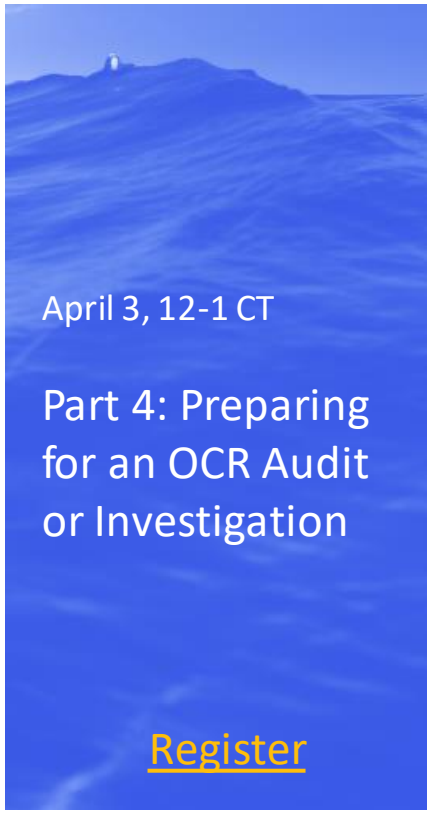
Register



March 27, 12-1 CT

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

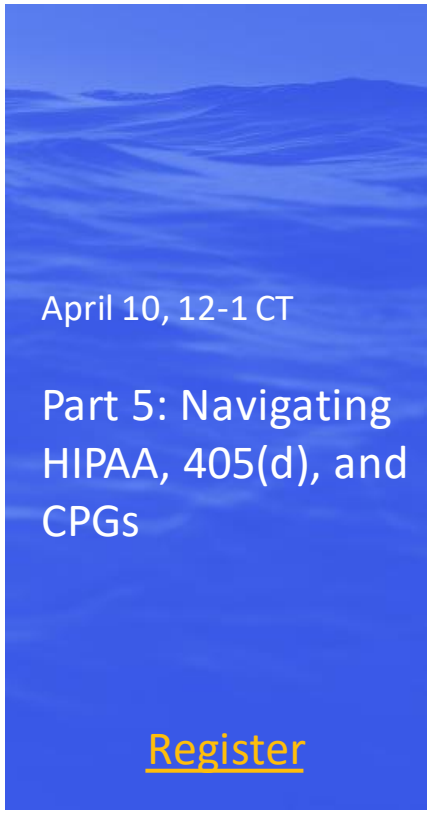
Register



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

HCCA | April 14-17

Stop by our booth (#300), and catch our speaking sessions:

- "How Safe Is 'Safe Harbor'? Balancing De-identification, Anonymization, and Pseudonymization of Health Data with Privacy Risks"
- "Beyond the Hype of AI and Tracking With a Focus on Ensuring Data Protection"

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.