# Preparing for an OCR Audit or Investigation

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
- What Happens During an Audit or Investigation?
- Preparing for an OCR Audit or Investigation
- Recommendations
- 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

# OCR's Authority Under HIPAA

- Office for Civil Rights (OCR) enforces the HIPAA Privacy and Security Rules by:
  - Investigating complaints filed with it
  - Conducting compliance reviews
  - Education and outreach to foster HIPAA compliance
  - 45 CFR §§ 160.306(c), 160.308, and 160.310(b)
- 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."
  - Phase I Audits (2011-2012) and Phase II Audits (2016-2017)

# Covered Entities and Business Associates

Covered Entities:

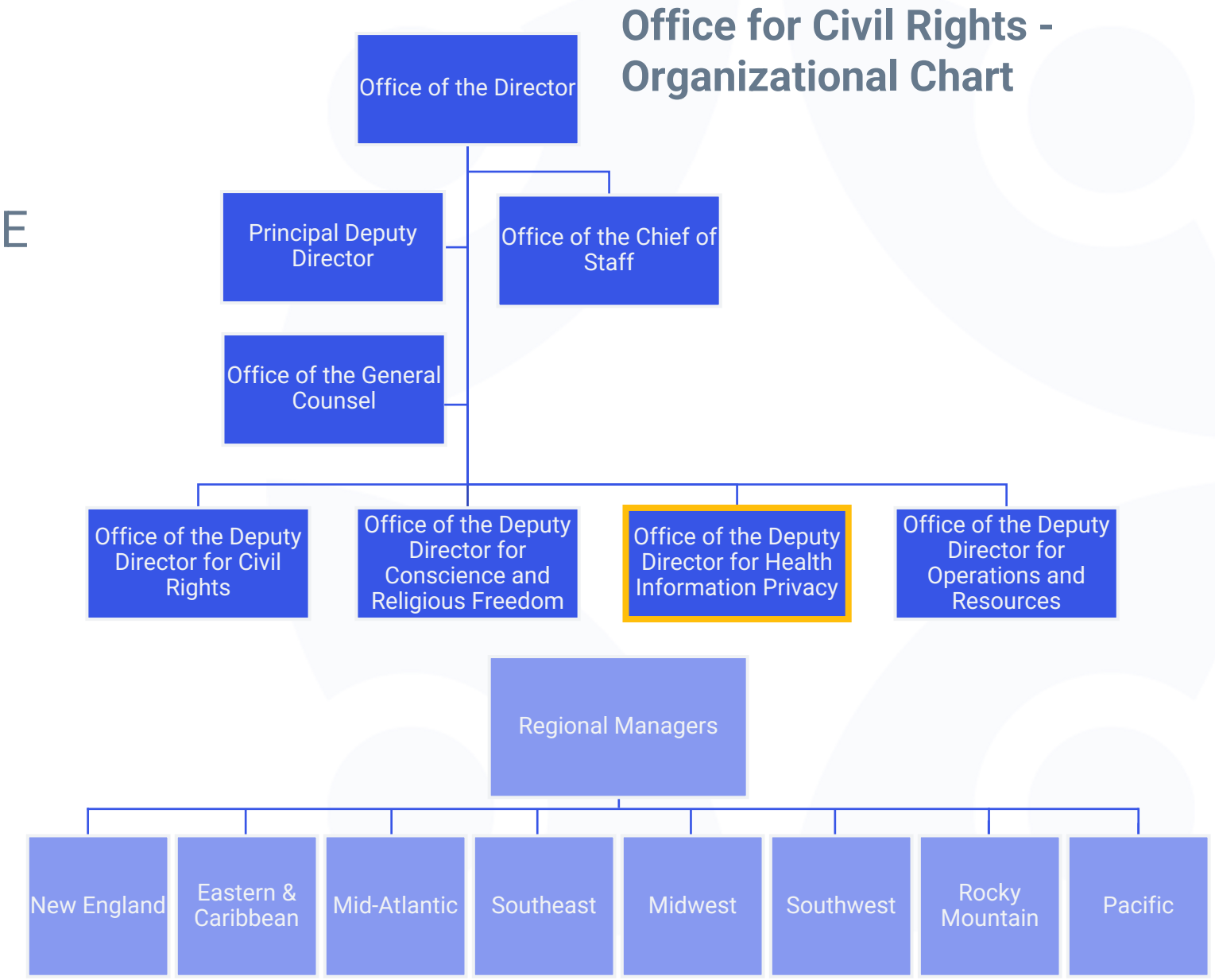
- a health plan, including but not limited to:
  - health insurance companies
  - company health plans
- a health care provider that electronically transmits any health information in connection with certain financial and administrative transactions (such as electronically billing insurance carriers for services)

Business Associates:

- a person (a natural person or a corporation or other entity) that creates, receives, maintains, or transmits protected health information (PHI) on behalf of a covered entity to perform certain functions, or provides certain services to or for a covered entity involving the disclosure of PHI

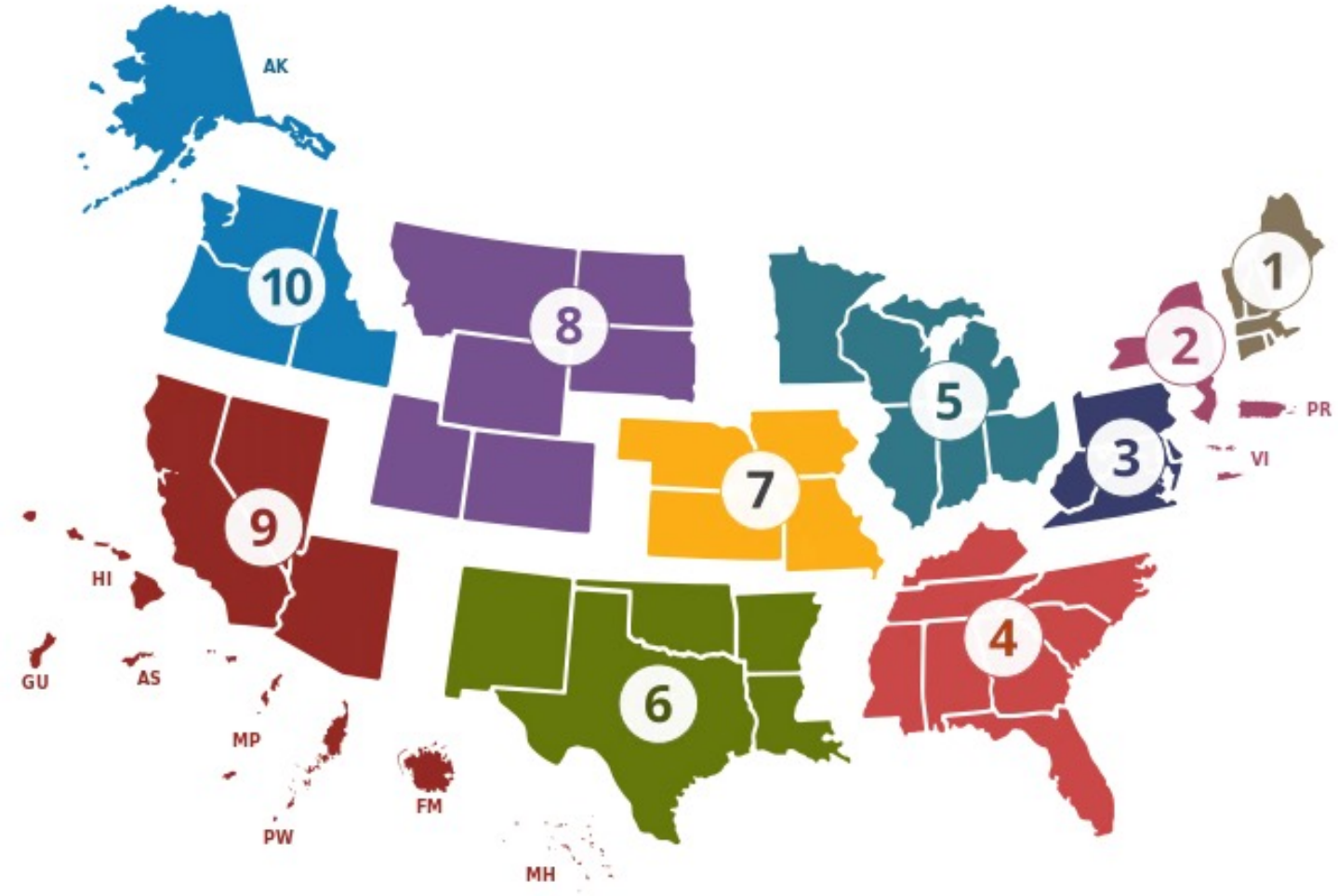
# Get to Know OCR!

- Personnel Tiers:
  - Investigator and/or SME
  - Advisor
  - Senior Advisor
  - Regional Manager
  - Deputy Director for Health Information Privacy
    - Timothy Noonan
  - Office of the Director
    - Melanie Fontes Rainer




Clearwater

# OCR Regional Map




Clearwater

# What Complaints will OCR Review?

- The alleged action must have occurred in the past 6 years
- Must be filed against a covered entity or a business associate
- Must allege an activity that, if proven true, would violate the HIPAA Rules
- Must be filed within 180 days of when the person submitting the complaint knew or should have known about the alleged violation of the HIPAA Rules
  - OCR may waive this time limit if individual shows good cause

# Data Request Example

**DEPARTMENT OF HEALTH & HUMAN SERVICES**
Voice - (404) 562-7886, (800) 368-1019
TDD - (404) 562-7884, (800) 537-7697
(FAX) - (404) 562-7881
http://www.hhs.gov/ocr/

**OFFICE OF THE SECRETARY**
Office for Civil Rights, Region IV
61 Forsyth Street, S. W.
Atlanta Federal Center, Suite 3B70
Atlanta, GA 30303-8909

January 28, 2008

[redacted]
Privacy Officer
[redacted]

Our Reference number: [redacted]

Dear Dr. Smith:

You were previously advised that the Department of Health and Human Services (HHS), Office for Civil Rights (OCR) has received a complaint on October 17, 2007 alleging that your office is not in compliance with certain aspects of the Federal Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164, Subparts A and E, the Privacy Rule) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Specifically, the complaint alleges that a patient, [redacted], has been unable to gain access to her complete medical records, even after several attempts. [redacted] alleges that she was only able to receive doctor's notes from two office visits. This allegation could reflect a violation of 45 C.F.R. § 164.524.

OCR enforces the Privacy Rule, and also enforces Federal civil rights laws that prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and, under certain circumstances, sex and religion.

Our authority to collect information and ascertain a covered entity's compliance is found at 45 C.F.R. §§ 160.300 - 160.316. As set forth in those provisions, to the extent practicable, OCR will seek the cooperation of covered entities in obtaining compliance with the applicable provisions of the Privacy Rule. A covered entity is required to submit records and compliance reports as may be necessary for OCR to ascertain whether the covered entity has complied with or is complying with the Privacy Rule.

The incident reported constitutes a potential violation of 45 C.F.R. § 164.524. In your fax sent to us on January 23, 2008, you indicated that you were not initially aware that [redacted] wanted a complete copy of her records. You further indicated that your office sent M[redacted]rt a complete copy of her records on January 22. While we are aware that [redacted] has received her medical records, OCR requests your cooperation in facilitating our review of this incident by asking that you provide all documentation listed in the attached Data Request Addendum. If you would fax these documents to Akara Whiten at (404) 562-7193, this would help to expedite the investigation.

**You will have 20 days from the day you receive this letter to respond and submit additional evidence as requested.** If we do not hear from you within those 20 days, and if OCR's investigation results in a finding that your practice is not complying with the Rule, HHS may initiate formal enforcement action which may result in the imposition of civil monetary penalties. We have previously sent you information explaining the penalty provisions under the Rule.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

Please be assured that our office is committed to resolving this matter in an efficient and timely manner. If you have any questions, please do not hesitate to contact Akara Whiten, Investigator, at (404) 562-7189 (Voice), (404) 331-2867 (TDD). When contacting this office, please remember to include the transaction number that we have given this file. That number is located in the upper left-hand corner of this letter.

Sincerely,

Roosevelt Freeman
Regional Manager

Enclosures: Data Request Addendum

Transaction number: 74086

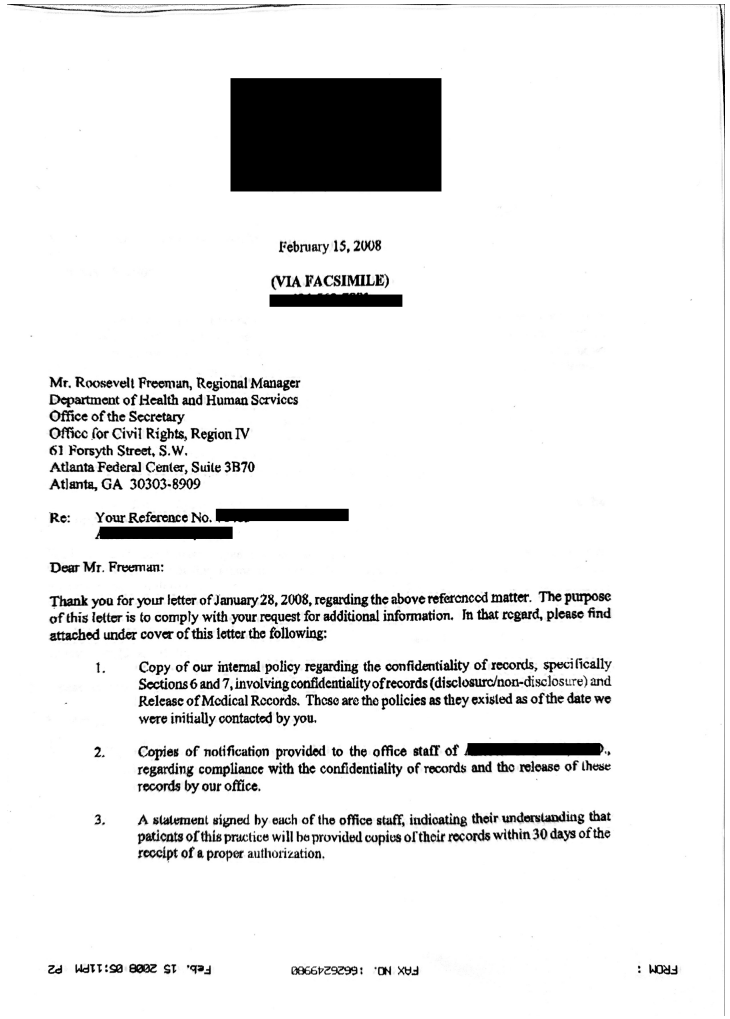
**DATA REQUEST**

1) Please submit a copy of your office's internal HIPAA Privacy Rule policies pertaining to **patient access of protected health information (§164.524)** as they currently exist. (Please submit only your policies as they relate to patient access because this is the sole issue raised in the complaint.)

2. In light of the allegation in this complaint, what steps, if any, have you taken to resolve any potential noncompliance with the Privacy Rule (such as additional staff training, redrafting of policies, employee sanctions)? Please provide us with documentation of one or more of the above measures.

3. Please reinforce with staff that you must provide patients with access to their records within 30 days of the request. Please provide documentation showing that all members of your staff understand this (i.e. a signed statement of understanding).

# Response Example



[redacted]

February 15, 2008

(VIA FACSIMILE)
[redacted]

Mr. Roosevelt Freeman, Regional Manager
Department of Health and Human Services
Office of the Secretary
Office for Civil Rights, Region IV
61 Forsyth Street, S.W.
Atlanta Federal Center, Suite 3B70
Atlanta, GA 30303-8909

Re: Your Reference No. [redacted]
[redacted]

Dear Mr. Freeman:

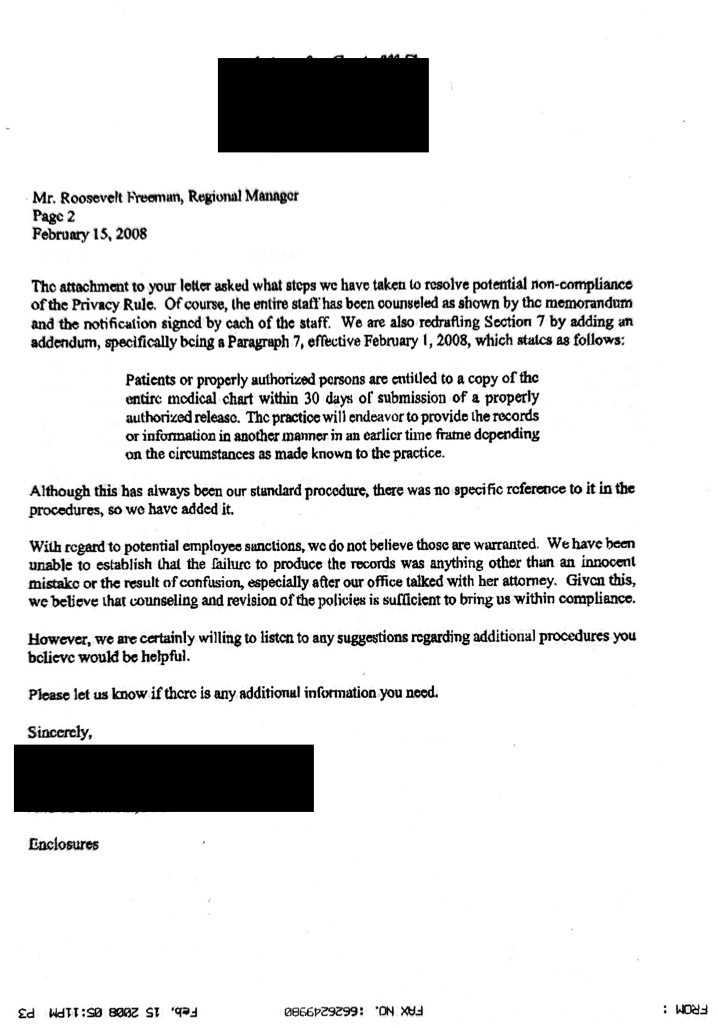
Thank you for your letter of January 28, 2008, regarding the above referenced matter. The purpose of this letter is to comply with your request for additional information. In that regard, please find attached under cover of this letter the following:

1. Copy of our internal policy regarding the confidentiality of records, specifically Sections 6 and 7, involving confidentiality of records (disclosure/non-disclosure) and Release of Medical Records. These are the policies as they existed as of the date we were initially contacted by you.

2. Copies of notification provided to the office staff of [redacted], regarding compliance with the confidentiality of records and the release of these records by our office.

3. A statement signed by each of the office staff, indicating their understanding that patients of this practice will be provided copies of their records within 30 days of the receipt of a proper authorization.

FROM : FAX NO. :6626249980 Feb. 15 2008 05:11PM P2



[redacted]

Mr. Roosevelt Freeman, Regional Manager
Page 2
February 15, 2008

The attachment to your letter asked what steps we have taken to resolve potential non-compliance of the Privacy Rule. Of course, the entire staff has been counseled as shown by the memorandum and the notification signed by each of the staff. We are also redrafting Section 7 by adding an addendum, specifically being a Paragraph 7, effective February 1, 2008, which states as follows:

> Patients or properly authorized persons are entitled to a copy of the entire medical chart within 30 days of submission of a properly authorized release. The practice will endeavor to provide the records or information in another manner in an earlier time frame depending on the circumstances as made known to the practice.

Although this has always been our standard procedure, there was no specific reference to it in the procedures, so we have added it.

With regard to potential employee sanctions, we do not believe those are warranted. We have been unable to establish that the failure to produce the records was anything other than an innocent mistake or the result of confusion, especially after our office talked with her attorney. Given this, we believe that counseling and revision of the policies is sufficient to bring us within compliance.

However, we are certainly willing to listen to any suggestions regarding additional procedures you believe would be helpful.

Please let us know if there is any additional information you need.

Sincerely,

[redacted]

Enclosures

FROM : FAX NO. :6626249980 Feb. 15 2008 05:11PM P3

Clearwater

# What Happens During an OCR Audit or Investigation?

# What is OCR's Formal Investigation Process?

- **Review** complaint; accept, deny, or refer (e.g., to CMS or DOE)
- **Notify** complainant and the covered entity named in complaint
- **Request** information about the complaint from the complainant and covered entity (15 - 30 days to reply)
- **Review** the information or evidence gathered
- **Determine** whether the covered entity violated HIPAA requirements
- **Resolve** mostly through:
  - Voluntary compliance, corrective action; and/or resolution agreement.
- **Notify** complainant and covered entity of the results

# Possible Investigation Outcomes

- OCR may impose civil money penalties (CMPs) if covered entity does not resolve the matter satisfactorily.
- Covered entity may request a hearing for review of case by an HHS administrative law judge.
- Complainants do not receive a portion of CMPs – the penalties are deposited in the U.S. Treasury.

# What an OCR Investigator Considers

- Analysis of each potential violation and possible conclusions
- Background research
- Identify claims that warrant further review
  - Additional data requests?
  - Onsite investigation?
- Early complaint resolution and voluntary compliance (i.e., parties agree on resolution and OCR closes the investigation)
- If no resolution…
  - Corrective action plan
  - Resolution agreement
  - Referral to Department of Justice or others

# 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 OCR's 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 provides draft findings and gave entities an opportunity to respond
7. OCR considers an entity's responses when preparing the entity's final report

# Investigator/Auditor Questions

- *Is the complaint complete?*
- *Is the complaint filed on behalf of a third party?*
- *Does OCR have the authority to investigate?*
- *Does the complaint allege a violation of the HIPAA Rules? Does it include sufficient information?*
- *Are there special sensitivities (consent to release identity, etc.)?*
- *Has complainant filed prior complaints against the CE or business associate?*
- *Was it filed on time?*
- *Does OCR have enough time to begin investigating?*
- *High impact case?*
- *Has the complaint been withdrawn?*

# Preparing for an OCR Audit or Investigation

# Preparing for an OCR Audit or Investigation

- Confirm the data request is from OCR:
  - Check the email address of the sender (should be “hhs.gov”)
  - Each data request letter has a “Transaction Number” – first two letters correspond to the year the data request is sent
  - Call the phone number listed on the complaint
  - Do a LinkedIn search for the investigator named in the complaint
  - Call or email OCR directly:
    - OCR’s contact page: https://www.hhs.gov/ocr/about-us/contact-us/index.html
      - Email OCRPrivacy@hhs.gov for Health Information Privacy questions
      - Contact regional offices (information on contact page)
  - The investigation may not be listed on the OCR Breach Portal

# Preparing for an OCR Audit or Investigation (cont.)

- Include/Invite the appropriate stakeholders
  - Legal representation
  - Digital forensics team
- Understand if onsite or desk investigation/audit
- Gather relevant documentation
  - Have relevant documentation/evidence readily available (digital and print)
- Craft an incident narrative
  - Summarize the alleged issue and the entity's response to the issue

# Recommendations

# Recommendations

- Confirm front line staff know how/where to send documents to OCR
- Don’t work in a vacuum
- Carefully read the letter/request
- Be respectful but don’t be afraid to clearly state when you believe something is incorrect (and can provide evidence to prove so)
- Respond in a timely fashion: answer data requests on time
- Communicate with the assigned investigator
- Request deadline extensions early
- Every case (and investigator) is different -- don't guess the case’s outcome based on the outcome of another case

# Conclusion

# Summary and Final Thoughts

- A compliance review, audit, or investigation from OCR is a possibility for every covered entity or business associate
- Accordingly, consider prioritizing being prepared for an OCR request and other regulatory inquiries in your organization
- Ensure that you are documenting evidence to support your organization's compliance with the HIPAA Privacy, Breach Notification, and Security Rules
- Partner with a 3rd party for a Mock OCR Audit and Mock OCR Investigation solutions to prepare your organization for such inquiries

# Q&A

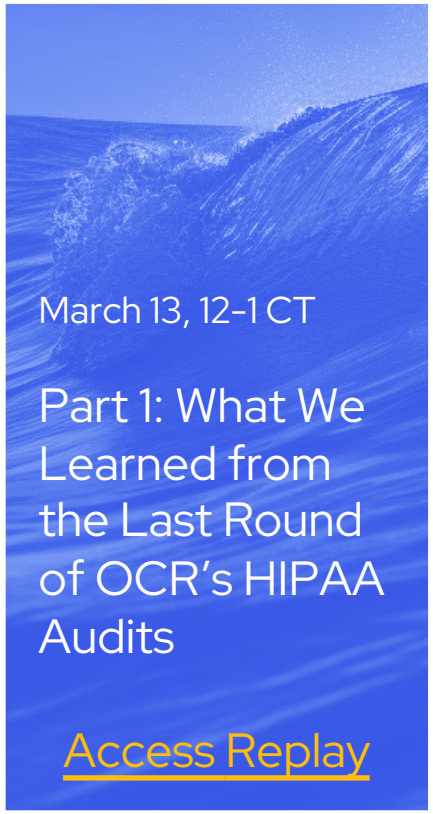
Andrew Mahler | Omenka Nwachukwu

# 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 Education

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



March 13, 12-1 CT

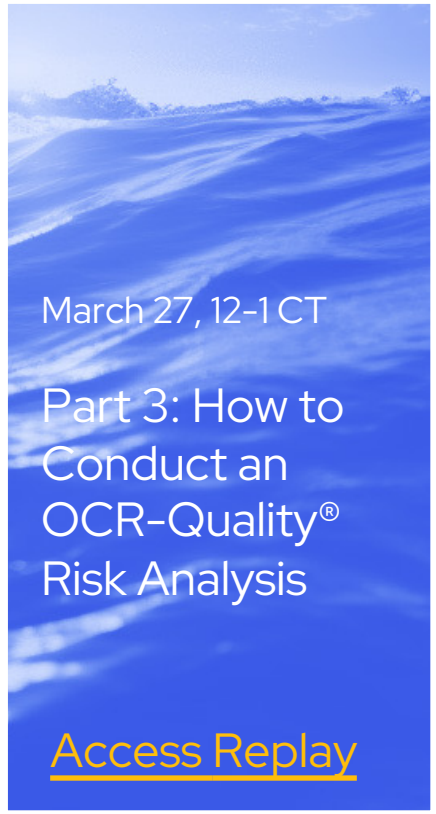
Part 1: What We Learned from the Last Round of OCR's HIPAA Audits

Access Replay

March 20, 12-1 CT

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

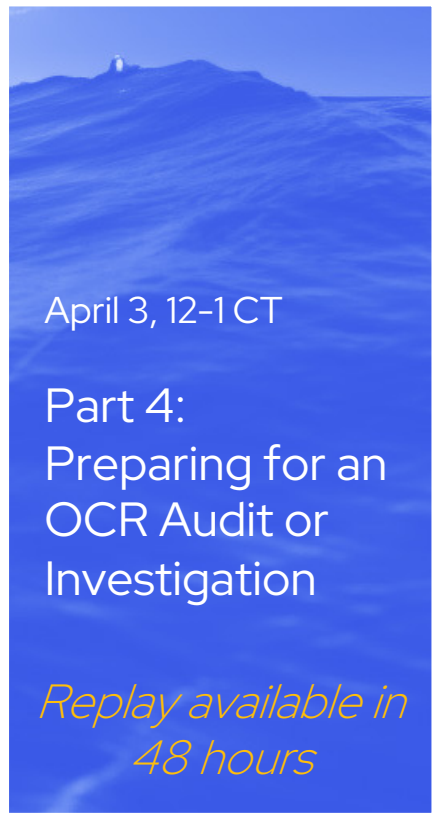
Access Replay



March 27, 12-1 CT

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

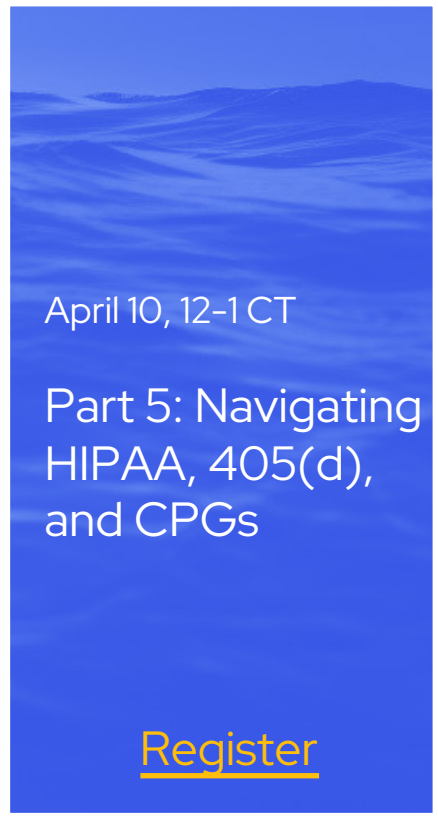
Access Replay



April 3, 12-1 CT

Part 4: Preparing for an OCR Audit or Investigation

*Replay available in 48 hours*



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

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Security & Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*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.