

HIPAA Security Rule NPRM: What to Know & What to Do

January 29, 2025

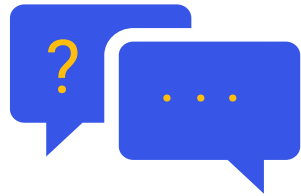


Meeting Logistics



Microphones

All attendees are on mute.



Questions

Type your questions in the Q&A box.



Resources

Upcoming events & resources linked.



Recording

Recording will be provided after event.



Survey

Survey will prompt at the end of webinar.

Agenda & Speakers

- Introductions
- Educational Content: HIPAA Security Rule NPRM: What to Know & What to Do
- Q+A
- Upcoming Events



Dave Bailey, EMBA, CISSP

Vice President, Consulting
Services, Security
Clearwater



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

Vice President, Consulting
Services, Privacy & Compliance
Clearwater

HIPAA Security Rule NPRM: What to Know & What to Do

Dave Bailey
Andrew Mahler



- Timelines
- Overview - NPRM to Strengthen Cybersecurity for ePHI
- Key Proposed Changes
- Proposed Administrative Safeguards
- Proposed Physical Safeguards
- Proposed Technical Safeguards
- Proposed Organizational Requirements
- Next Steps
- Q&A

NPRM Timeline

NPRM Issued December 27, 2024



Public Comment Period Ends March 7, 2025

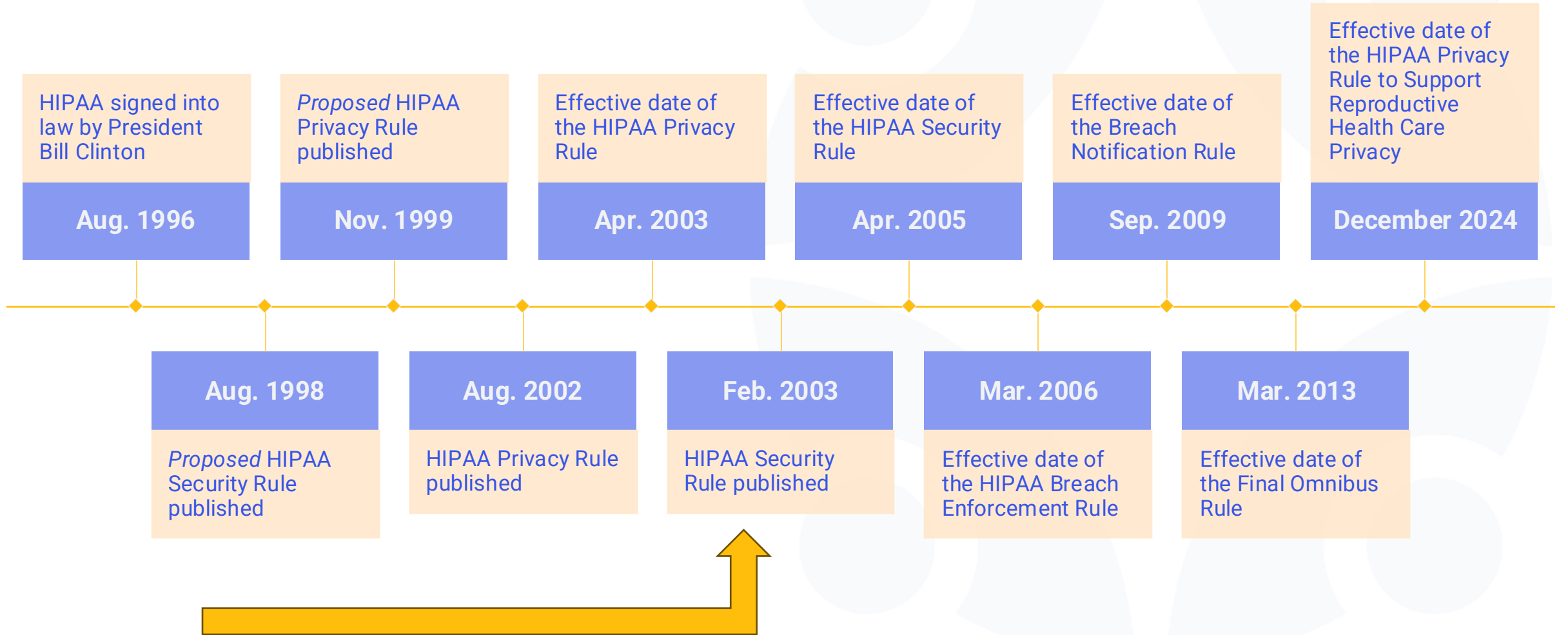


Effective Date is 60 Days After Final Rule is Published



Compliance Date is 240 Days After the Effective Date

Background - Timeline





Overview - NPRM to Strengthen Cybersecurity of ePHI



Healthcare Sector is Struggling with Effective Security

- Threats to the sector are growing exponentially, impacting patient safety and creating financial hardships
- The NPRM solidifies and emphasizes critical and necessary cybersecurity practices and required controls to safeguard patients and patient data
- The NPRM consistently refers to guidance and alignment to NIST, Health Industry Cybersecurity Practices 404(d), and the HHS Cybersecurity Performance Goals (CPGs)





Cyberattacks continue to impact the health care sector, with rampant escalation in ransomware and hacking causing significant increases in the number of large breaches reported to OCR annually...

The number of people affected every year has skyrocketed exponentially, a number we expect to grow even bigger this year with the Change Healthcare breach, the largest breach in our health care system in U.S. history.

This proposed rule...would require updates to existing cybersecurity safeguards to reflect advances in technology and cybersecurity, and help ensure that [those] providing health care meet their obligations to protect the security of individuals' protected health information across the nation.

- OCR Director Melanie Fontes Rainer (August 2022 - January 2025)

Background – What Was Considered

Advisory recommendations and strategies

Enforcement and recurring compliance issues (ex. 2019 – 2023: 89% increase in hacking; 102% increase in ransomware)

Large-scale disruptions

Proposals, laws, and enforcement at federal and state level

Inconsistent use of cybersecurity best practices

Increased risk to ePHI posed by AI and emerging technologies

Need for regulatory clarity as result of litigation

Overall changes to health care environment since 2003



Key Proposed Changes



Key Proposed Changes

The NPRM proposes to strengthen the Security Rule's standards and implementation specifications with new proposals and clarifications

- Clarifies scope: all systems that create, receive, transmit or maintain ePHI, connected systems, or systems that contain information that could provide access or threaten those systems
- Removal of the distinction between the “required” and “addressable” implementation specifications, making all implementation specifications mandatory, with specific, limited exceptions
- Detailed specifications for the risk analysis requirement
- Requires regulated entities to maintain technology asset inventory and map
- Strengthens requirements for planning for contingencies and responding to security incidents
- Requires compliance audits every 12 months
- Requires implementation, deployment and testing of technical controls every 12 months
- Require business associates to notify covered entities upon activation of contingency plan

Takeaway:

The proposed rule seeks to strengthen cybersecurity by updating the Security Rule's standards to better address ever-increasing cybersecurity threats to the health care sector.

Proposed New Terms and Modifications

Proposed new terms

Deploy, Implement, Electronic Information System, Multi-factor Authentication, **Relevant Electronic Information System**, Risk, Technical controls, Technology Asset, Threat, Vulnerability

Proposed modifications

Access, Administrative Safeguards, Authentication, Availability, Confidentiality, Information System, Malicious Software, Password, Physical Safeguards, Security or Security Measures, Security Incident, Technical Safeguards, User, **Workstation**



Proposed Administrative Safeguards



Demonstrate you know all your systems, where your data is, where it goes, and how many vendors are in the mix

Administrative Safeguards – Technology Asset Inventory

- 1 Maintain a system inventory of all in-scope information systems and technology assets; Establish a written inventory
- 2 Maintain a network map documenting the flow of ePHI that includes transfers to third party systems or business associates; reviewed and updated minimally every 12 months and when there is a change in the environment or operations that may affect ePHI

Takeaway:

Gone is the notion of managed vs unmanaged; it all must become managed and secured within the scope of protected health information enclave



“Regulated entities cannot understand the risks to the confidentiality, integrity, and availability of their ePHI without a complete understanding of these assets...the inventory forms the foundation for a fulsome and accurate risk analysis.”

Once you complete your inventory conduct a risk analysis to adequately protect the CIA of ePHI

Conduct a risk analysis that is compliant with the Security Rule

- 1 Review the technology asset inventory and the network map to identify where ePHI may be created, received, maintained, or transmitted within its information systems
- 2 Identify reasonably anticipated threats to the CIA of ePHI
- 3 Identify potential vulnerabilities and predisposing conditions
- 4 Create an assessment and documentation of the security measures
- 5 Determine the likelihood that a threat would exploit a vulnerability
- 6 Determine the impact of a threat exploiting a vulnerability
- 7 Create an assessment of risk level for each identified threat and vulnerability
- 8 Create an assessment of risks to ePHI posed by entering into or continuing a business associate agreement

Current risk analysis methodology aligns with current OCR Guidance and is validated in the proposed NPRM

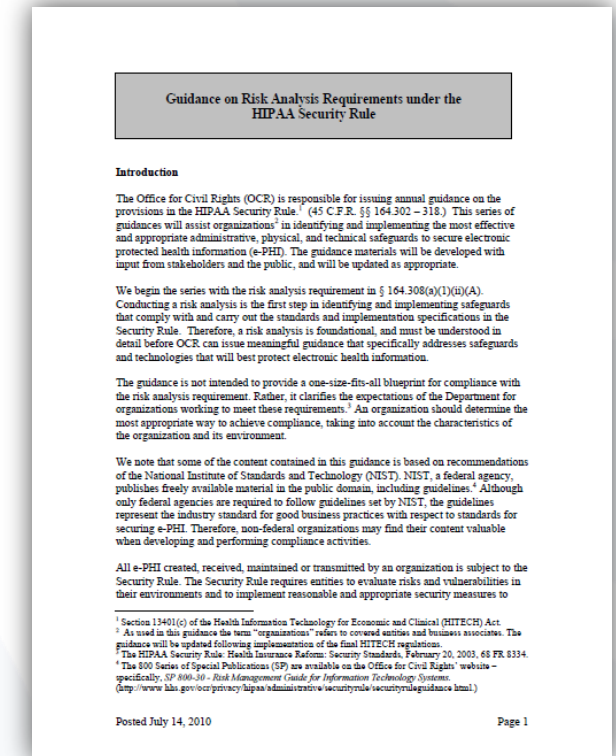
The new definition of risk analysis in the proposed Rule aligns very well with Clearwater's methodology. Clearwater was pleased to see OCR adopt terms and concepts that Clearwater has historically incorporated into its risk analysis such as "technology asset" and "component"

D. Section 164.308(a)(2)(i)—Standard: Risk Analysis

"After a regulated entity conducts a written inventory of its technology assets and creates its network map, it is critical for it to identify the potential risks and vulnerabilities to its ePHI. Conducting a risk analysis is necessary to adequately protect the confidentiality, integrity, and availability of ePHI"

"Other NIST guidance on conducting risk assessments explains that the result of a risk analysis is a determination of risk posed to the regulated entity's ePHI and related information systems."

OCR Guidance on Risk Analysis



Healthcare organizations that follow best practices for risk management are less likely to have an impactful security incident.

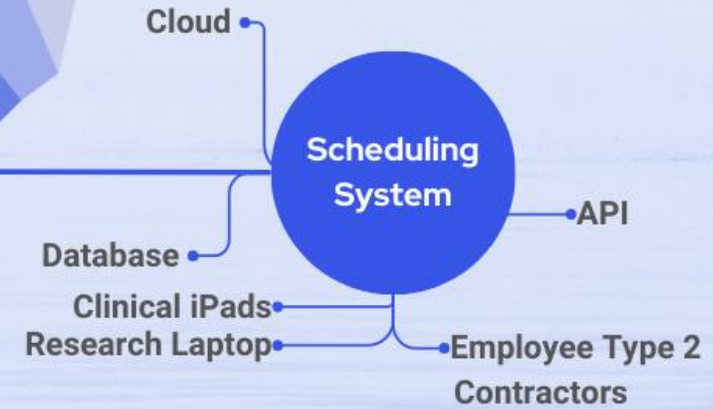
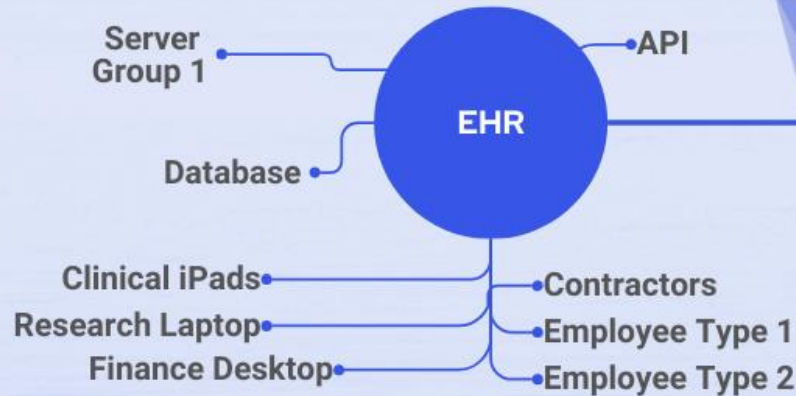
What does “good” look like?

- Inventory systems with ePHI and define impact level
- Assess foundational controls and implementation of controls at the asset level
- Conduct Asset & Component level Risk Analysis (Likelihood x Impact)
- Document risk treatment decisions
- Create and document actionable risk mitigation plans that optimize risk reduction
- Track mitigation progress and report to governing body
- Update risk analysis as changes occur



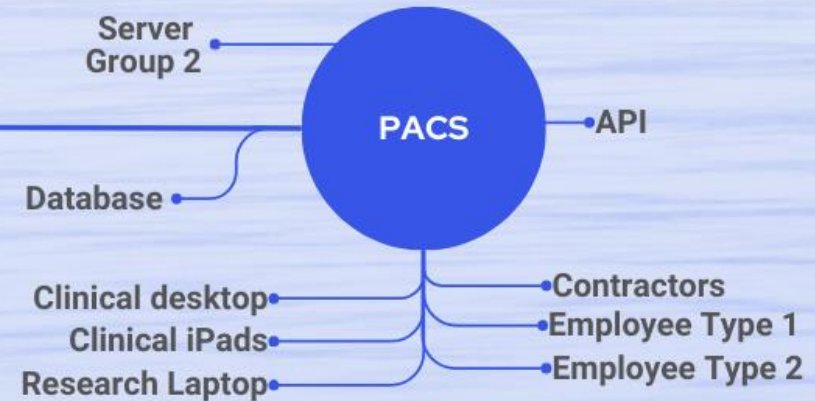
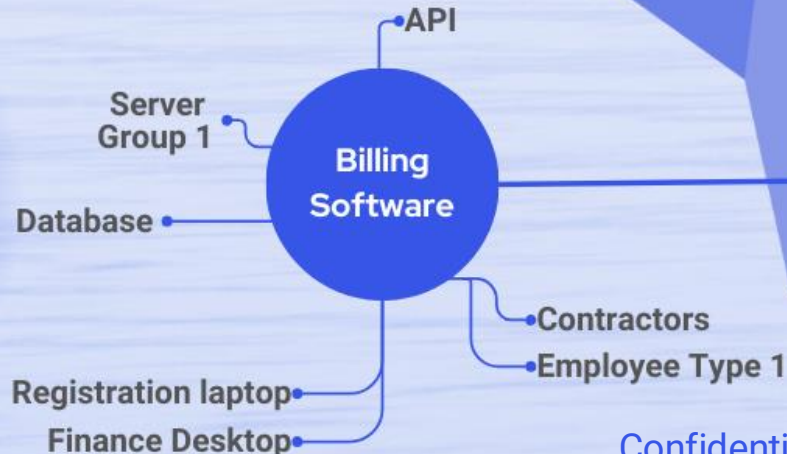
Traditional Risk Analysis

NIST Risk Management Tiers 1 & 2



Asset-Based Risk Analysis

NIST Risk Management Tier 3



Workforce Security – Proposed Requirements

“Good security practices entail continuous awareness, assessment, and action in the face of changing circumstances.”

- 1 Establish and implement written procedures for terminating a workforce member's access to ePHI and relevant electronic information systems; review and test every 12 months
- 2 Require that the workforce member's access be terminated as soon as possible, but no later than one hour after the workforce member's employment or other arrangement ends
- 3 Require notification to another regulated entity after a change in or termination of a workforce member's authorization to access ePHI as soon as possible, but no later than 24 hours after the authorization to access ePHI or relevant electronic information systems is changed or terminated

To Consider:

- **“Establish clear job descriptions and responsibilities and identifying in writing who has the business need and who has been granted permission to view, alter, retrieve, and store ePHI and at what times, under what circumstances, and for what purposes”**

Business Associates – Proposed Requirements

A problem: the current Security Rule does not require a regulated entity to verify that entities that create, receive, maintain, or transmit ePHI on its behalf are taking the necessary steps to protect that ePHI

- 1 Require a business associate to both report to a covered entity or another business associate activation of its contingency plan within 24 hours of such activation and report known or suspected security incidents
- 2 Require the regulated entity to obtain written verification from the business associate that the business associate has deployed the required technical safeguards every 12 months
- 3 Require that the written verification be accompanied by a written certification by a person who has the authority to act on behalf of the business associate that the analysis has been performed and is accurate

Takeaway:

- **Does not change reporting requirements**
- **Would require BAA revisions**

Proposed Administrative Safeguards - Highlights

Patch Management

- Within “a reasonable and appropriate period of time” or “within 15 calendar days of identifying the need to address a critical risk where a patch, update, or upgrade is available; or within 15 calendar days of a patch, update, or upgrade becoming available.”

Risk Management

- Proposal aligns with HHS’ essential CPG to Mitigate Known Vulnerabilities
- Establish and implement a written risk management plan for reducing risks to all ePHI

Information System Activity Review

- Implement written policies and procedures for regularly reviewing records of activity in its relevant electronic information systems
- Retain records of activity
- Respond to a suspected or known security incident identified during the review of activity in accordance with the security incident plan

Proposed Administrative Safeguards - Highlights

Information Access Management

- Verification of the identities of users and technology assets prior to accessing relevant electronic information systems, including MFA technical controls
- Ensure that relevant electronic information systems are segmented to limit access to ePHI to authorized workstations

Contingency Plan

- Perform and document an assessment of the relative criticality of its relevant electronic information systems and technology assets
- Written procedures to restore both its critical relevant electronic information systems and data within 72 hours of the loss, and to restore the loss of other relevant electronic information systems and data in accordance with its criticality analysis

Compliance Audit

- Requirement to perform and document an audit of the compliance with each standard and implementation specification of the Security Rule at least once every 12 months



Proposed Physical Safeguards



Proposed Physical Safeguards

Clarifies that physical safeguards be applied to all ePHI throughout the regulated entity's facilities, remove any distinction between addressable and required implementation specifications, and modify all four physical safeguard standards to require that the requisite policies and procedures be in writing and implemented throughout the enterprise

- 1 Facility Access Controls
- 2 Workstation Use and Security
- 3 Technology Asset Controls

To Consider:

- In writing?
- Procedures for role-based access to facilities?
- Procedures for security cameras?
- Removal and movement of workstations?



Proposed Technical Safeguards



Required means Required

The NPRM highlights critical cybersecurity practices that are necessary; however, have been challenging to implement

- 1 Encryption at rest and in transit
- 2 Multifactor Authentication
- 3 Network Segmentation
- 4 Security Configuration Baselines
- 5 Vulnerability scanning at least every six months and penetration testing at least once every 12 months
- 6 Separate technical controls for backup and recovery of ePHI and relevant electronic information systems
- 7 Review and test the effectiveness of certain security measures at least once every 12 months

All implementation specifications are mandatory, with limited exceptions



Proposed Organizational Requirements



Proposed Organizational Requirements - Highlights

Group Health Plans

- Require that plan documents of the group health plan would obligate a plan sponsor or any agent to whom it provides ePHI to implement the administrative, physical, and technical safeguards of the Security Rule
- Require plan documents to include a provision requiring a plan sponsor to report to the group health plan without unreasonable delay, but no later than 24 hours after activation of its contingency plan

Documentation Requirements

- Require policies and procedures implemented to comply with the Security Rule, and as part of that documentation, explain how it considered the reasonable and appropriate measures
- Document all the actions, activities, and assessments required by the Security Rule
- Update its documentation at least once every 12 months and within a reasonable and appropriate period of time after a security measure is modified

New and Emerging Technologies

- Before implementing new and emerging technologies, a regulated entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
- Quantum computing
- AI
- VR/AR



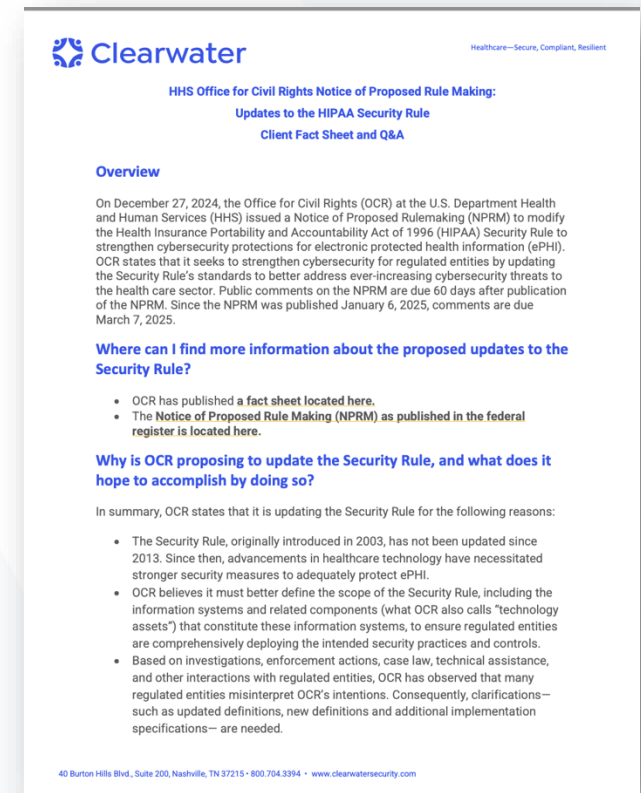
Next Steps



Clearwater team of experts evaluating proposed changes

- Clearwater published fact sheet and Q&A
 - Feedback is welcome on the NPRM, and we are evaluating whether to submit comments during the public comment period
 - We will continue to provide updates to our clients as more information is known and our review of the NPRM is complete
 - A formal assessment of the proposed rule is not required at this time; however, we can assist if desired

HHS Office for Civil Rights Notice of Proposed Rule Making: Updates to the HIPAA Security Rule Client Fact Sheet and Q&A





Q&A



Upcoming Events



ViVE | February 16-19, 2025 Nashville, TN

- Clearwater is excited to again serve as title sponsor of the Cybersecurity Pavilion as the ViVE conference returns to Nashville in early 2025.
- Steve Akers, CTO & CISO, Clearwater will be speaking in the Cybersecurity Pavillion Stage
- [Click here](#) for more information and to book a meeting with us



HIMSS Global Conference March 3-6, 2025 Las Vegas, NV

- **Session Time:** Tuesday, March 4 at 10:15am PT **Session Title:** "Mastering Cyber Threat Intelligence to Protect Patient Safety".
- **Speakers:** Jon Moore, Clearwater Chief Risk Officer and Head of Consulting Services & Client Success & Michal Gross, Manager of Cybersecurity Intelligence for the Cleveland Clinic
- [Click here](#) for more information and to book a meeting with us



HPE Miami 2025 March 5-6, 2025 Miami, FL

- Stop by Clearwater's dedicated meeting table in the networking lounge to connect with our team of experts—Baxter Lee, CFO, David Kolb, Sales VP, and Richmond Donnelly, Sr. Account Executive.
- [Click here](#) for more information and to book a meeting with us



ADSO Summit 2025 March 16-19, 2025 San Diego, CA

- Be sure to stop by the Clearwater Kiosk to meet our team, including John Howlett, CMO & SVP and David Anderson, Sr. Account Executive.
- [Click here](#) for more information and to book a meeting with us

Upcoming Webinars



Guiding the Future: A Board Member's Framework for Managing AI Risks | Feb 4 @ 1:00 CST

- Join Jon Moore, Chief Risk Officer at Clearwater, for this essential webinar designed specifically for healthcare board members of The Governance Institute.
- This session will equip board members with the tools to navigate the complexities of AI, enhance organizational resilience, and oversee AI deployment that benefits both employees and patients while adhering to regulatory and ethical standards.
- [Click here](#) for more information and to register



Clearwater's Monthly Cyber Briefing | The Return of OCR Audits: What It Means and How to Prepare for Potential Action | Feb 6, 2025 @ 12:00 CST

- This session features Steve Cagle, CEO, Clearwater as well as Andrew Mahler, VP Consulting Services, Clearwater and Iliana Peters, Shareholder at Polsinelli
- The Monthly Cyber Briefing is a digest of trending news and announcements related to healthcare's cybersecurity landscape
- [Click here](#) for more information and to register



Forty-Second National HIPAA Summit | March 25-28, 2025 – Virtual

- Clearwater is thrilled to participate and speak in 4 different sessions in the Virtual HIPAA Summit happening March 25-28, 2025! This event brings together top professionals and thought leaders in healthcare compliance, cybersecurity, and privacy to tackle the most pressing issues in healthcare today.
- [Click here](#) for our speaking sessions and to register



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/](https://www.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

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.



Appendix - Current Trends



Breach Reports via OCR Breach Portal

OCR Breach Portal Data¹

- 706 breach reports totaling 184.5M individual records, an increase of 10% over 2023
- Top 10 Breaches of 2024 represented 84% of reported records breached

Healthcare Records Breached²



Top 10 Breaches of 2024

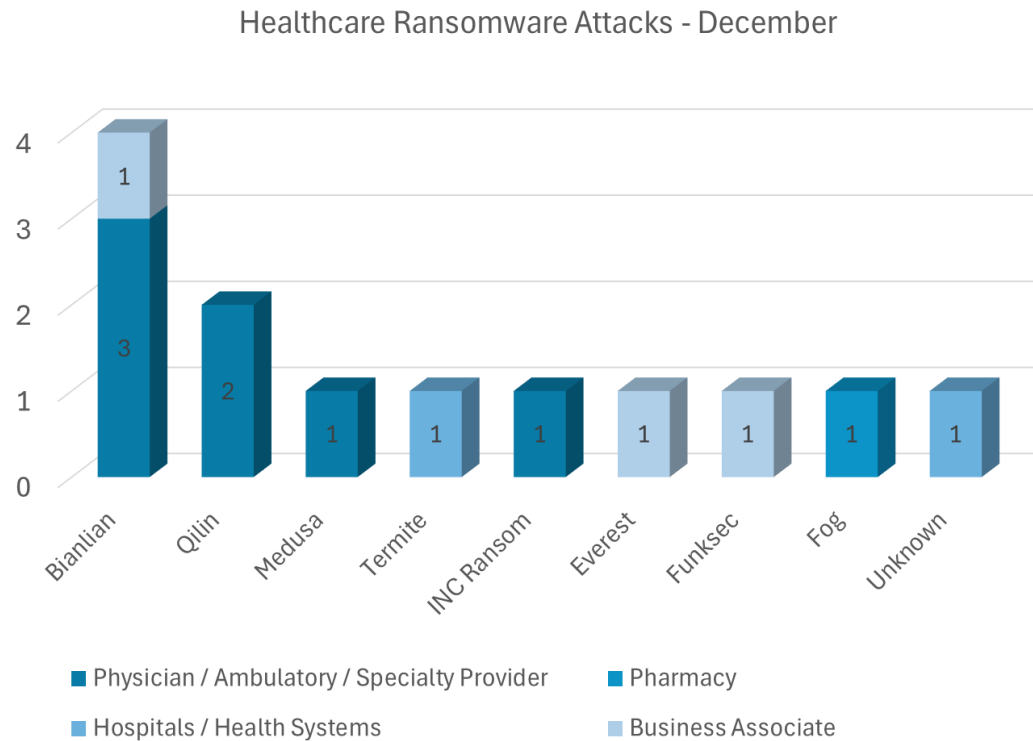
Regulated Entity	Records
Change Healthcare, Inc.	100,000,000
Kaiser Foundation Health Plan, Inc.	13,400,000
Ascension Health	5,599,699
HealthEquity, Inc.	4,300,000
Concentra Health Services, Inc.	3,998,163
CMS	3,112,815
Acadian Ambulance Service, Inc.	2,896,985
A&A Services d/b/a Sav-Rx	2,812,336
WebTPA Employer Services, LLC	2,518,533
INTEGRIS Health	2,385,646
Total	141,024,177

¹ The [HHS Breach Portal](#) (2024 data through 12/31/24, pulled on 1/6/25; 2023 data pulled 11/3/24)

² [Rocky Mountain Gastroenterology Reportedly Experiences Triple Cyberattack, Resulting in Data Breach Affecting Up to 169k | Console and Associates, P.C. - JDSupra](#)

Ransomware Attacks

December was a particularly difficult month for Healthcare sector as existing and emerging threat actors continued to target hospitals, physician groups and healthcare services organizations.



- At least 18 known attacks in the healthcare sector in December
- As reported last month, we continue to see specialty care / physician management groups highly targeted
- Multiple attacks on California Hospitals over last 45 days
- In 2024 118 confirmed and 147 unconfirmed ransomware attacks took place in the US healthcare sector costing the industry \$21.9B.³

Source: [Halcyon Attacks Lookout](#) (December ransomware attacks as reported on 12/27/24)

¹ [California hospital recovers from cyber attack after nearly 2 weeks](#)

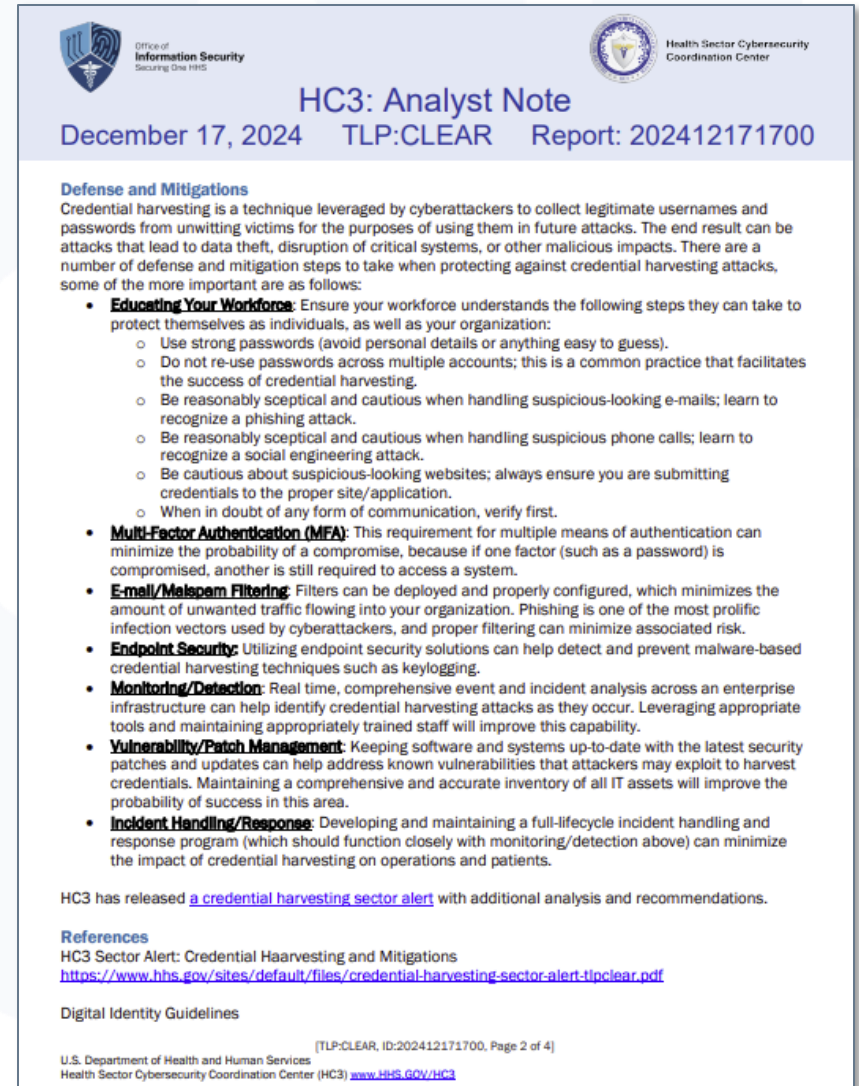
² [Cyber criminals claim they hacked 17 million patient records at PIH Health hospitals – Daily News](#)

³ Source: [Comparitech](#)

HC3 Alert – Credential Harvesting

The Health Sector Cybersecurity Community Center (HC3) issued an alert about on-going credential harvesting campaigns targeting the healthcare sector.

- Specific campaigns targeting healthcare and other industries
- Techniques employed
 - Phishing
 - Man in the Middle
 - Key logging
 - Credential Stuffing
 - Social Engineering
 - Phony Login Pages
 - Malware
- *Credential phishing attacks increased by 703% and social engineering attacks 141% in 2nd half 2024¹*



The screenshot shows a document titled "HC3: Analyst Note" dated December 17, 2024, with TLP: CLEAR and Report ID: 202412171700. It is issued by the Office of Information Security (Securing the HHS) and the Health Sector Cybersecurity Coordination Center. The document discusses "Defense and Mitigations" for credential harvesting, defining it as a technique where cyberattackers collect legitimate usernames and passwords from unwitting victims. It lists several defense and mitigation steps:

- Educating Your Workforce:** Ensure your workforce understands the following steps they can take to protect themselves as individuals, as well as your organization:
 - Use strong passwords (avoid personal details or anything easy to guess).
 - Do not re-use passwords across multiple accounts; this is a common practice that facilitates the success of credential harvesting.
 - Be reasonably sceptical and cautious when handling suspicious-looking e-mails; learn to recognize a phishing attack.
 - Be reasonably sceptical and cautious when handling suspicious phone calls; learn to recognize a social engineering attack.
 - Be cautious about suspicious-looking websites; always ensure you are submitting credentials to the proper site/application.
 - When in doubt of any form of communication, verify first.
- Multi-Factor Authentication (MFA):** This requirement for multiple means of authentication can minimize the probability of a compromise, because if one factor (such as a password) is compromised, another is still required to access a system.
- E-mail/Malspam Filtering:** Filters can be deployed and properly configured, which minimizes the amount of unwanted traffic flowing into your organization. Phishing is one of the most prolific infection vectors used by cyberattackers, and proper filtering can minimize associated risk.
- Endpoint Security:** Utilizing endpoint security solutions can help detect and prevent malware-based credential harvesting techniques such as keylogging.
- Monitoring/Detection:** Real time, comprehensive event and incident analysis across an enterprise infrastructure can help identify credential harvesting attacks as they occur. Leveraging appropriate tools and maintaining appropriately trained staff will improve this capability.
- Vulnerability/Patch Management:** Keeping software and systems up-to-date with the latest security patches and updates can help address known vulnerabilities that attackers may exploit to harvest credentials. Maintaining a comprehensive and accurate inventory of all IT assets will improve the probability of success in this area.
- Incident Handling/Response:** Developing and maintaining a full-lifecycle incident handling and response program (which should function closely with monitoring/detection above) can minimize the impact of credential harvesting on operations and patients.

HC3 has released [a credential harvesting sector alert](#) with additional analysis and recommendations.

References
HC3 Sector Alert: Credential Harvesting and Mitigations
<https://www.hhs.gov/sites/default/files/credential-harvesting-sector-alert-tlpclear.pdf>

Digital Identity Guidelines

[TLP: CLEAR, ID: 202412171700, Page 2 of 4]
U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3) www.HHS.GOV/HC3

OCR Begins 2024-2025 Auditing Program

OCR continues enforcement for breach and ransomware HIPAA violations. Additionally, it has initiated the 2024 – 2025 Audit program previously announced.

2024-2025 HIPAA Audits Initiated

OCR has initiated its 2024-2025 HIPAA Audits. Ransomware, destructive malware, and other forms of malicious hacking present a growing and ongoing threat to the U.S. health care and public health sector and the privacy and security of electronic protected health information. In recent years, HIPAA covered entities (health plans, health care clearinghouses, and most health care providers) and business associates have experienced significant cyberattacks, which have impacted hospital operations, patient care, access to patient records and have had massive financial ramifications. Substantial increases in large breaches involving hacking and ransomware reported to OCR and the number of individuals affected by large breaches demonstrates the need for HIPAA covered entities and their business associates to ensure that they are complying with the HIPAA Security Rule.

The 2024-2025 HIPAA Audits will review 50 covered entities' and business associates' compliance with selected provisions of the HIPAA Security Rule most relevant to hacking and ransomware attacks.

December 4, 2024

HHS Office for Civil Rights Imposes a \$1.19 Million Penalty Against Gulf Coast Pain Consultants for HIPAA Security Rule Violations

December 6, 2024

HHS Office for Civil Rights Imposes a \$548,265 Penalty Against Children's Hospital Colorado for HIPAA Privacy and Security Rules Violations