

# Monthly Cyber Briefing

March 2024



# 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 & Speakers

- Cyber update
- Change Healthcare update and focus on third-party risk



Steve Cagle  
CEO  
Clearwater



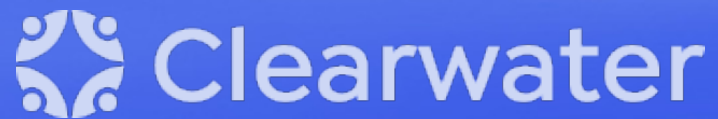
Dave Bailey  
VP, Consulting Services  
Clearwater



Andrew Mahler  
VP, Privacy and Compliance  
Clearwater

# Cyber Update

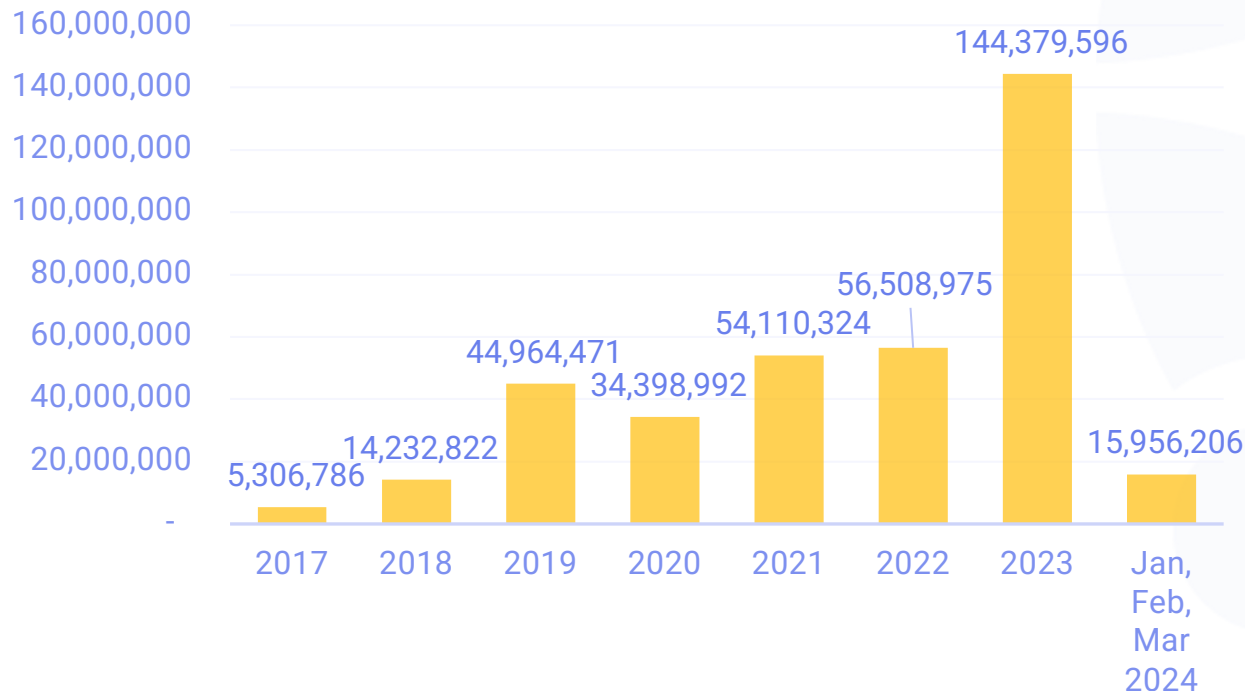
Steve Cagle



# Breach Reports via OCR Breach Portal<sup>1</sup>

- 144.4M records reported breached in 2023, an increase of 61% vs 56.5 million in 2022
- 737 breaches reported in 2023 vs 720 in 2022, a slight increase year over year
- OCR added additional breaches and/or updates to number of records in 2023, increasing records breached by 10 million

Healthcare Records Reported as Breached



## Notable in March 2024 breach data

- About 16 million records (167 breaches) reported Jan – March.
- 76% of breaches were due to hacking incidents
- No breach data from last week of March available on the portal as of 4/1/24
- There was only one breach greater than 500,000 records reported – Emergency Medical Services Associates<sup>2</sup>

<sup>1</sup>HHS Breach Portal (data pulled March 3, 2024).

<sup>2</sup>Refer to March Cyber Briefing for top breaches of 2025

# Change Healthcare - Updates

- UnitedHealthcare has confirmed data was stolen and says it is trying to determine what sensitive data was breached
- U.S. State Department offers \$10m award for information related to capture of BlackCat/ALPHV
- HHS ASPR sends letter detailing how to get information from health plans regarding payment “flexibility” options
- Relay Exchange, the largest exchange, was back online last week; however, many systems still not reconnected

[Link to Active Payer List – Reconnected](#)

[Link to Change Healthcare Status Updates](#)

[Link to System Status](#)



The image shows a letter from the U.S. Department of Health and Human Services (HHS), the Administration for Strategic Preparedness and Response (ASPR), and the Centers for Medicare & Medicaid Services (CMS), dated March 25, 2024. The letter is addressed to the healthcare provider community and discusses the impacts of a cyberattack against Change Healthcare, including disrupted billing and claims operations. It mentions that the Biden-Harris Administration is leading with solutions, providing flexibility for state Medicaid programs to provide interim payments to fee-for-service providers, making advance and accelerated payments available to providers and hospitals through Medicare, and urging health plans to do the same. The letter also mentions that the U.S. State Department offers a \$10m award for information related to the capture of BlackCat/ALPHV. The letter is signed by Andrea Palm, Deputy Secretary, and Dawn Adams, Administrator.

Below the letter is a screenshot of a system status dashboard for Change Healthcare Enterprise. The dashboard lists various systems and their status:

System	Status
Clinical Decision Support	
CareSelect®	✓
InterQual® AutoReview	✓
InterQual® Cloud Solutions	⚠
InterQual® Coordinated Care	✓
InterQual® Criteria	✓
InterQual® Customize	✗
InterQual® Review Manager – Hosted	⚠
InterQual® Review Manager – Installed	✓
Patient Education	✓
InterQual® Government Services	✗
Clinical Network	
Clinical Document Collector API	✗
Clinical Exchange	✗
Clinical Exchange Channel Partners including ePrescribe and Orders & Results	✗
Clinical Exchange Labs and Hospitals	✗
CommonWell	✓

# Is it Safe To Reconnect?

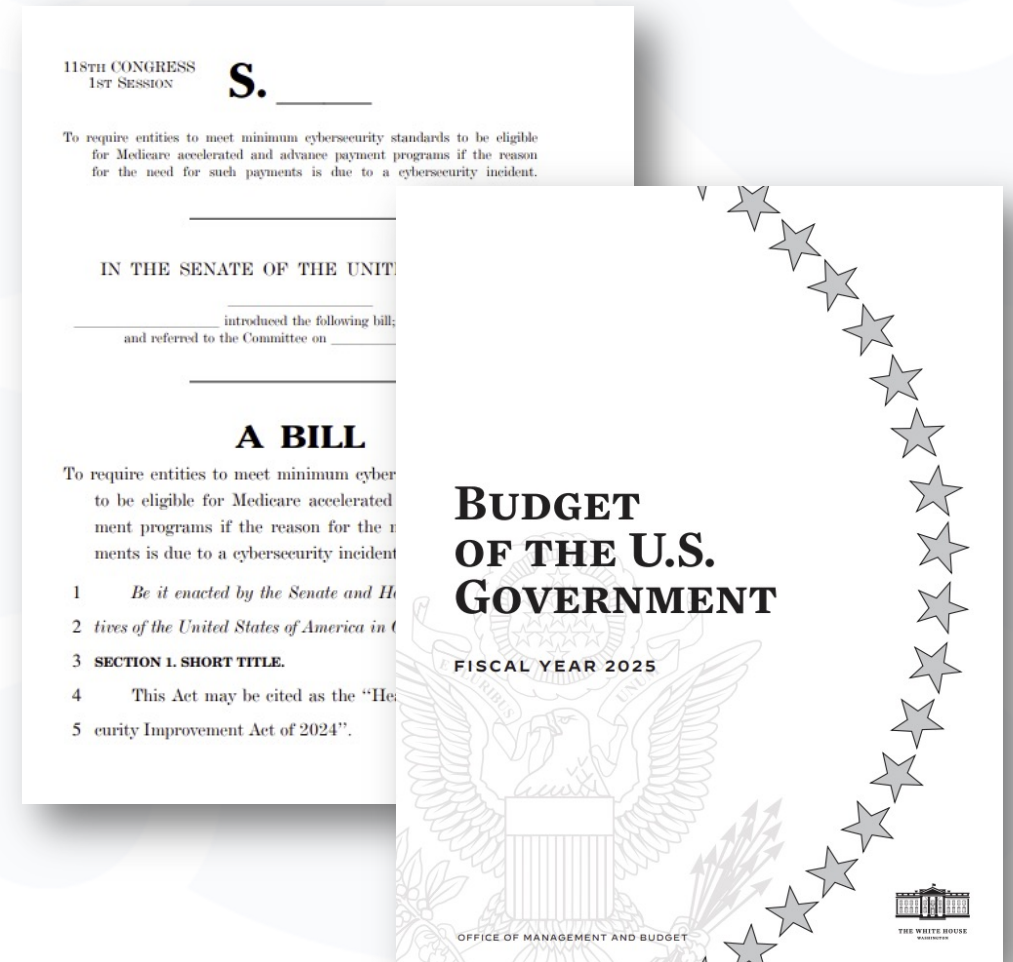
Here are some of the security steps that Change said it took while restoring Relay Exchange and Assurance services

- Restored systems across accounts from clean backups.
- Trend Micro, completed scanning prior to services going into production.
- Amazon's Guard Duty used to complete the initial scanning post restoration.
- Palo Alto's Unit 42 scanned the environment for malicious activity
- Change Healthcare also conducted vulnerability scans via Tenable.
- Bishop Fox penetration tested external-facing endpoints.
- Servers supporting Assurance and Relay Exchange were re-scanned by Mandiant and confirmed cleared prior to moving the servers to production.
- Documentation from Bishop Fox, Mandiant and UHG were made available for customers reconnecting to the service.

*"We remain confident in what our telemetry and controls demonstrated – that our Optum UnitedHealthcare and UnitedHealth Group systems are safe and were not affected by this issue."*


# Minimum Cybersecurity Standards for Healthcare Proposed & Biden Administration 2025 Budget Calls for More Funding

- [New bill](#) proposed by Senator Warner would allow for advance and accelerated payments to providers in the event of a cybersecurity incident, so long as they meet minimum cybersecurity standards
  - Bill modifies the existing Medicare Hospital Accelerated Payment Program and the Medicare Part B Advance Payment Program
  - No mention of what the standards are or how it would be determined that they were met
- [2025 Biden administration budget proposal](#) for cybersecurity
  - \$3B for CISA (increase of \$103M)
  - \$800 million for high need hospitals for basic cybersecurity defenses
  - \$500 million incentive program for all hospitals
  - \$141 million for HHS own security





# CIRCIA Rule Proposed

 This document is scheduled to be published in the Federal Register on 04/04/2024 and available online at <https://federalregister.gov/2024-06524>, and on <https://govinfo.gov> DE 9110-G1

**DEPARTMENT OF HOMELAND SECURITY**  
Cybersecurity and Infrastructure Security Agency  
6 CFR Part 226  
[Docket No. CISA-2022-0010]  
RIN 1670-AA04  
**Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements**  
AGENCY: Cybersecurity and Infrastructure Security Agency, DHS  
ACTION: Proposed rule.  
SUMMARY: The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, requires the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities. CISA seeks comment on the proposed rule to implement CIRCIA's requirements and on several practical and policy issues related to the implementation of these new reporting requirements.  
DATES: Comments and related material must be submitted on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].  
ADDRESSES: You may send comments, identified by docket number CISA-2022-0010, through the Federal eRulemaking Portal available at <http://www.regulations.gov>.  
Instructions: All comments received must include the docket number for this rulemaking. All comments received will be posted to <https://www.regulations.gov>, including any personal information provided. If you cannot submit your comment using <https://www.regulations.gov>, contact the person in the FOR FURTHER INFORMATION

Cyber Incident Reporting for Critical Infrastructure Act of 2022 – or CIRCIA - intended to help the agency prevent cyberattacks and deploy assistance to victims

- Applies to 16 critical infrastructure industries
- Proposes to include hospitals with more than 100 beds and critical access hospitals, pharmaceutical manufacturers, and manufacturers of Class II and Class III devices
- Proposes to excludes Labs/diagnostics, payors, and health IT companies (but may change after comment period)
- Requires report of a “substantial” cyber incident within 72 hours and a ransomware payment within 24 hours
- 60 days for comments
- Rule to go into effect no later than 18 months from March 27<sup>th</sup>.

# HHS OCR Updates Tracking Technologies Guidance

## Key Updates

- Doubles down on its position that online tracking technologies must comply with HIPAA regulations
- Modifies position on “unauthorized” user – if intention is to seek healthcare than included, otherwise not considered included (Question – How would one know the intention?)
- Clarifies position on mobile apps, and transfer of PHI – it is included
- Maintains its position that if a tracking technology vendor meets the definition of a business associate under HIPAA, a regulated entity should establish a BAA with that vendor
- States enforcement priority

### Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

*On March 18, 2024, OCR updated this guidance to increase clarity for regulated entities and the public.*

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities<sup>1</sup> and business associates<sup>2</sup> (“regulated entities”) under the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) when using online tracking technologies (“tracking technologies”).<sup>3</sup> OCR administers and enforces the HIPAA Rules, including by investigating breach reports and complaints about regulated entities’ noncompliance with the HIPAA Rules. A regulated entity’s failure to comply with the HIPAA Rules may result in a civil money penalty.<sup>4</sup>

Tracking technologies are used to collect and analyze information about how users interact with regulated entities’ websites or mobile applications (“apps”). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity’s health care operations.<sup>5</sup> The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI).<sup>6</sup> Some regulated entities may share sensitive information with tracking technology vendors and such sharing may involve unauthorized disclosures of PHI with such vendors.<sup>7</sup> **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures<sup>8</sup> of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.<sup>9</sup>

An impermissible disclosure of an individual’s PHI not only violates the Privacy Rule<sup>10</sup> but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual’s PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.

While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, OCR is providing this reminder that it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.

# HC3 Sector Alerts

Office of Information Security  
Securing Our HHS

Health Sector Cybersecurity  
Coordination Center


## HC3: Sector Alert

March 12, 2024 TLP:CLEAR Report: 202403121700

### Defense and Mitigations from E-mail Bombing

**Overview**  
E-mail bombing, also known as mail bomb or letter bomb attacks, occur when a botnet (a single actor or group of actors) flood an e-mail address or server with hundreds to thousands of e-mail messages. They are a type of Denial of Service (DoS) attack that allows attackers to bury legitimate transaction and security messages in an unsuspecting inbox by rendering the victim's mailbox useless. By overloading a victim's inbox, attackers hope that a victim will miss important e-mails like account sign-in attempts, updates to contact information, financial transaction details, or online order confirmations.

This type of attack is of particular importance to the Healthcare and Public Health (HPH) sector. In 2016, unknown assailants launched a massive cyber attack aimed at flooding thousands of targeted ".gov" (.gov) e-mail inboxes with subscription requests, rendering many unusable for days. E-mail bombs are not only an inconvenience to the victim, but to everyone using that particular server. When an e-mail server is impacted by a DDoS, it can downgrade network performance and potentially lead to direct business downtime. This Sector Alert provides an overview of types of e-mail bomb techniques, as well as defenses and mitigations for targets of this type of attack.



**Figure 1:** Signs of a bot-driven Denial-of-Service attack. (Source: TechTarget)

**Types of E-mail Bombs**  
**Registration Bombs:** While e-mail bombing attack methods vary, most attacks use legitimate newsletter sign-ups from normal websites. The e-mail utilizes automated bots, which crawl the web, searching for newsletter sign-up pages or forms that do not require a form of live-user authentication. Attackers maintain lists of these vulnerable sites, and some will even advertise how often they update their attack lists.

Once the e-mail bomb order is placed, scheduled, and begins, the bots will sign an unlucky recipient up for all of these newsletters at once. This generates thousands of e-mails arriving to the victim immediately. Beside the immediate impact, victims receive an annoying, steady flow of unwanted e-mails that will keep arriving years after the initial attack. To add further frustration, the victim is added to additional spam, phishing, and malware lists by malicious actors. Since the bombs originate from numerous sources, this type is a Distributed Denial of Service attack (DDoS).

[TLP:CLEAR, ID#202403121700, Page 1 of 8]  
U.S. Department of Health and Human Services  
Health Sector Cybersecurity Coordination Center (HC3) [www.HHS.GOV/HC3](http://www.HHS.GOV/HC3)

## March 12 – Email Bombing



## March 18 – Credential Harvesting and Mitigation



Office of Information Security  
Securing Our HHS

Health Sector Cybersecurity  
Coordination Center

## HC3: Sector Alert

March 18, 2024 TLP:CLEAR Report: 202403181500

### Credential Harvesting and Mitigations

**Executive Summary**  
Cyberattacks against healthcare facilities can involve credential harvesting, which may lead to a disruption of operations. Credential harvesting, also known as credential stealing or credential phishing, is a technique that cybercriminals can use to obtain sensitive login credentials like usernames, passwords, and personal information. These credentials operate as the gateway to an individual's digital identity, and can grant access to various types of information, such as online accounts and health data. The methods employed for credential harvesting are diverse, ranging from sophisticated phishing emails to fake websites and social engineering tactics.

**Report**  
The healthcare sector commonly makes use of digital technologies to manage patient data, streamline operations, and enhance medical services. Credential harvesting refers to the process of stealing user authentication credentials for malicious purposes. Attackers can employ various techniques to obtain these credentials, including phishing, keylogging, and brute force attacks. Once acquired, these credentials can be used to gain unauthorized access to sensitive data, systems, or networks. There are multiple ways attackers can accomplish credential harvesting, and their goal is to convince a user to enter their login credentials into a malicious outlet, enabling the attacker access to the user's account.

- **Phishing:** Phishing attacks involve sending deceptive emails or messages that appear to be from legitimate sources. These emails aim to trick users into providing their login credentials on fake websites or through other means.
- **Keylogging:** Keyloggers are malicious software or hardware that record keystrokes entered by users, capturing sensitive information such as usernames and passwords.
- **Brute Force Attacks:** In brute force attacks, attackers systematically try numerous combinations of usernames and passwords until they discover the correct credentials to access a system or account.
- **Person-in-the-Middle (PITM) Attacks:** In PITM attacks, hackers intercept communication between two parties, capturing login credentials exchanged during the authentication process.
- **Credential Stuffing:** Attackers use previously compromised credentials to gain unauthorized access to other accounts where users have recycled the same username and password.

Credential harvesting can lead to data breaches, exposing patients' confidential information, including medical records, personal details, and other types of data. These breaches are capable of impacting patient privacy, and can negatively impact healthcare operations by giving an attacker access to deploy malware or conduct other nefarious operations. Accessing healthcare systems through credential harvesting can disrupt critical services, such as patient care delivery and administrative functions. System downtime and compromised infrastructure can impede medical professionals' abilities to access essential resources and provide timely care.

**Impact to the HPH Sector**  
Credential harvesting is capable of disrupting normal operations, impeding the delivery of vital services and patient care. When systems are compromised, entities may experience downtime, inability to access

[TLP:CLEAR, ID#202403181500, Page 1 of 3]  
U.S. Department of Health and Human Services  
Health Sector Cybersecurity Coordination Center (HC3) [www.HHS.GOV/HC3](http://www.HHS.GOV/HC3)

# HC3 – February Vulnerability Summary

- Summarizes key vulnerabilities “of interest” to the Health Sector
- Includes recently published vulnerabilities related to Connectwise, Ivanti, Google/Android, Apple, Mozilla, Cisco, SAP, VMWare, Adobe, Fortinet, Atlassian
- HC3 recommends that all healthcare entities review their Known Exploited Vulnerabilities Catalog, a living list of known CVEs that carry significant risk to the U.S. federal enterprise

The screenshot shows the top portion of a report titled "HC3: Monthly Cybersecurity Vulnerability Bulletin" dated March 19, 2024. The report is from the Office of Information Security, Department of Health and Human Services, and the Health Sector Cybersecurity Coordination Center. The report ID is 202403191500. The main heading is "February Vulnerabilities of Interest to the Health Sector". The text explains that in February 2024, vulnerabilities to the health sector have been released, including the monthly Patch Tuesday vulnerabilities. It lists vendors such as Ivanti, ConnectWise, Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, VMware, Adobe, Fortinet, and Atlassian. It notes that a vulnerability is classified as a zero-day when it is actively exploited with no fix available or if it is publicly disclosed. HC3 recommends patching all vulnerabilities, with special consideration for the risk management posture of the organization. The report also includes a section on the importance to the HPH Sector, a section from the Department of Homeland Security/Cybersecurity & Infrastructure Security Agency (CISA) regarding the Known Exploited Vulnerabilities Catalog, and a section on Ivanti vulnerabilities, including a security update and a joint advisory on threat actors exploiting these vulnerabilities. It lists CVEs CVE-2024-46805, CVE-2024-21887, and CVE-2024-21893. The report concludes with additional information on previously mentioned vulnerabilities and a footer with the report ID and a URL to the report.

Office of Information Security  
Securing Our HHS

Health Sector Cybersecurity Coordination Center

## HC3: Monthly Cybersecurity Vulnerability Bulletin

March 19, 2024 TLP:CLEAR Report: 202403191500

### February Vulnerabilities of Interest to the Health Sector

In February 2024, vulnerabilities to the health sector have been released that require attention. This includes the monthly Patch Tuesday vulnerabilities released by several vendors on the second Tuesday of each month, along with mitigation steps and patches. Vulnerabilities for February are from Ivanti, ConnectWise, Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, VMware, Adobe, Fortinet, and Atlassian. A vulnerability is given the classification of a zero-day when it is actively exploited with no fix available or if it is publicly disclosed. HC3 recommends patching all vulnerabilities, with special consideration given to the risk management posture of the organization.

#### Importance to the HPH Sector

#### Department Of Homeland Security/Cybersecurity & Infrastructure Security Agency

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) added a total of 9 vulnerabilities to their [Known Exploited Vulnerabilities Catalog](#). This effort is driven by [Binding Operational Directive \(BOD\) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities](#), which established the Known Exploited Vulnerabilities Catalog as a living list of known CVEs that carry significant risk to the U.S. federal enterprise. Vulnerabilities that are entered into this catalog are required to be patched by their associated deadline by all U.S. executive agencies. While these requirements do not extend to the private sector, HC3 recommends that all healthcare entities review the vulnerabilities in this catalog and consider prioritizing them as part of their risk mitigation plan. The full database can be found [here](#).

#### Ivanti

Ivanti released a [security update](#) regarding the Ivanti Connect Secure and Ivanti Policy Secure Gateways, which gained a lot of attention in January. Additionally, CISA released a [joint advisory on threat actors exploiting these vulnerabilities](#). According to the advisory, cyber threat actors have exploited flaws in Connect Secure and Policy Secure, which are tracked as CVE-2024-46805, CVE-2024-21887, and CVE-2024-21893, where the threat actors can exploit a chain to bypass authentication, craft malicious requests, and execute arbitrary commands with elevated privileges. CISA also relayed the following two key findings:

- The Ivanti Integrity Checker Tool is not sufficient to detect compromise due to the ability of threat actors to deceive it, and
- A cyber threat actor may be able to gain root-level persistence despite the victim having issued factory resets on the Ivanti device.

Additional information on the previously mentioned vulnerabilities can be found below:

- [CVE-2023-46805](#): An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.
- [CVE-2024-21887](#): A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.

[TLP:CLEAR, ID# 202403191500, Page 1 of 7]

U.S. Department of Health and Human Services  
Health Sector Cybersecurity Coordination Center (HC3) [www.HHS.GOV/HC3](http://www.HHS.GOV/HC3)

# How is Our Sector Responding to the Change Healthcare Incident?

*The Change Healthcare ransomware attack has been a “wake up” call to many in the healthcare sector*

- CEOs and Boards are devoting significant, personal attention to cybersecurity
- Many are calling for more regulation and / or more financial support for under-resourced entities
- Updating their risk analysis and importantly - increasing scope, and going deeper to the information asset and component level in their assessments
- Re-allocating budget to long de-prioritized cybersecurity investments that contribute to high risks
- Improving their monitoring, detection and response capabilities
- Bolstering resiliency: performing business impact analysis, updating and testing incident response plans
- Enhancing their vendor risk management programs
  - Reactive: conducting more frequent monitoring of their high impact vendors, and more validation
  - Proactive: Assessing their entire 3<sup>rd</sup> party cyber risk management program

# 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<sup>®</sup> Compliance Program

[Access Replay](#)

March 27, 12-1 CT

Part 3: How to Conduct an OCR-Quality<sup>®</sup> Risk Analysis

[Access Replay](#)

April 3, 12-1 CT

Part 4: Preparing for an OCR Audit or Investigation

[Replay coming soon](#)

April 10, 12-1 CT

Part 5: Navigating HIPAA, 405(d), and CPGs

[Register](#)

# Change Healthcare Update and Third- Party Risk

Dave Bailey



# Change Healthcare +43 Days; Top Concerns

## Business Impact

- How many vendors can cause the same/similar impact the Change cyber attack has caused?
- Does your Business Impact Analysis and the Business Continuity Plan provide effective recovery and ability to return to normal operations?
- What is needed to improve the security of the HPH as part of Critical Infrastructure Protection

## Third Party Risk

- Is the current method to assess vendor risk adequate?
- How can we receive timely and actionable information on a vendor's security posture?

## Risk Tolerance

- Does your organization understand its risk tolerance?
- Are the stakeholders identified and known on who pulls the plug, and who gives the green light to turn on?
- If the Change incident impacts your data, are you prepared with expected next steps?

## Vulnerability & Threat Management

- Are you receiving and acting on alerts from vendors & relevant sources?
- Once a vulnerability is known, how quickly can you patch and remediate?
- Is there confidence in the effectiveness of implemented controls and response and recovery plans?



# Relevant Threat Indicators

- HC3: Sector Alert March 18<sup>th</sup>, 2024: Credential Harvesting and Mitigations:
  - Credential harvesting refers to the process of stealing user authentication credentials for malicious purposes
- There are multiple ways attackers can accomplish credential harvesting, and their goal is to convince a user to enter their login credentials into a malicious outlet, enabling the attacker access to the user's account.

## Recorded Future 2024 Predictions



The “phishing” landscape will become the “spearfishing” landscape as generative AI helps attackers create particularized lures.

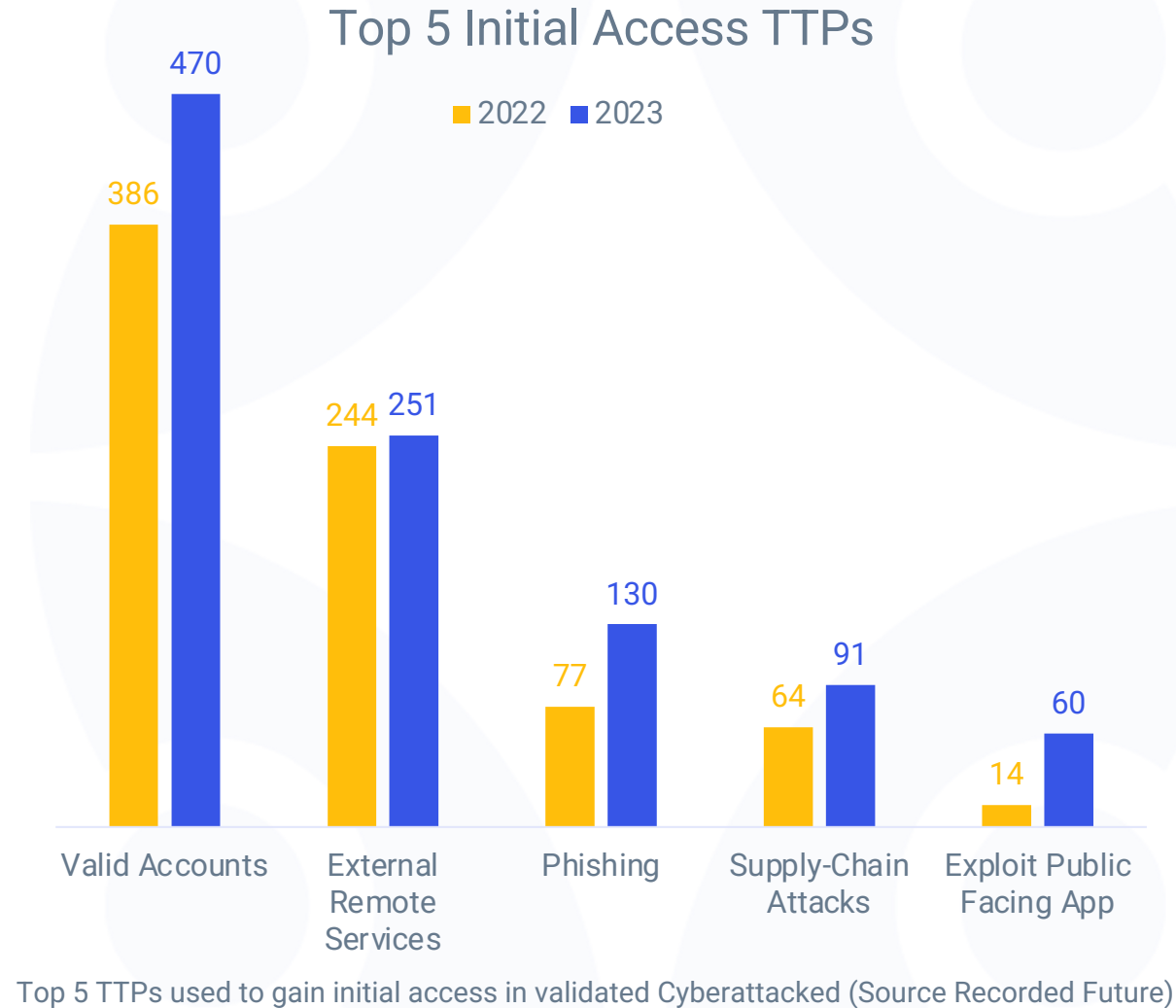


The rise of passwordless logins will likely drive criminal activity away from infostealers and back to email-based credential harvesting.

2023 Annual Report: Recorded Future, March 21, 2024

# Tactics of the Adversary

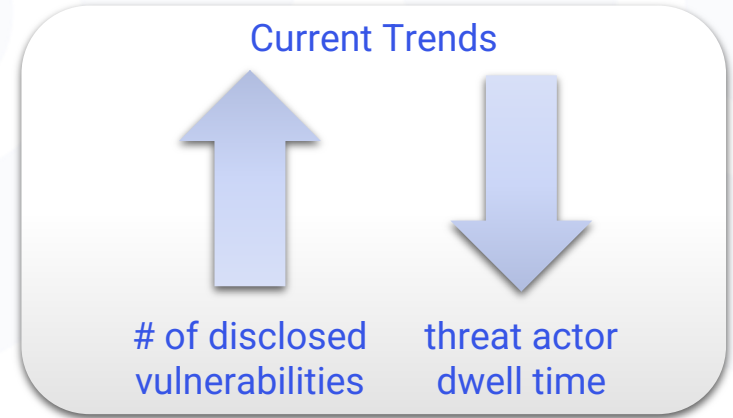
- The individual continues to be the target of the adversary to steal credentials and exploit **vulnerabilities in third-party services**



# 2023 Top Exploited Vulnerabilities

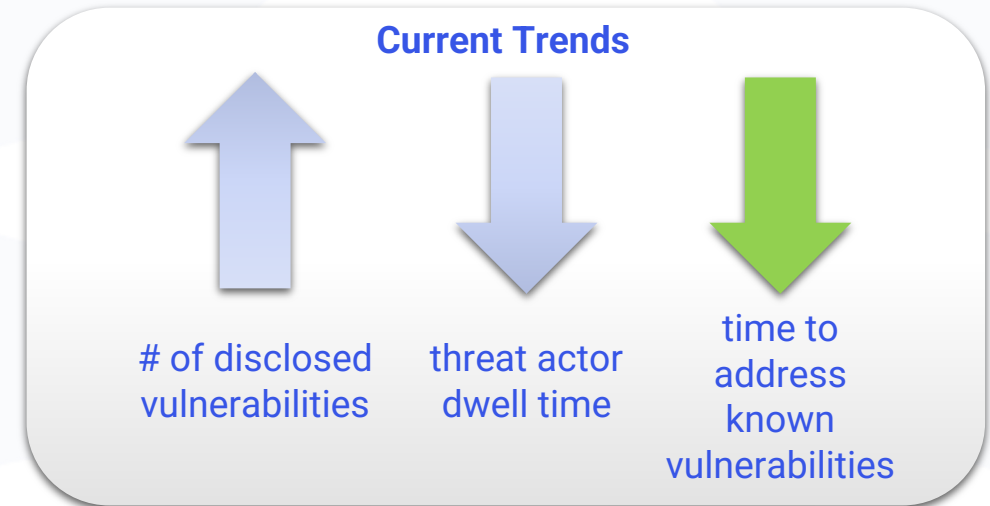
- CVE-2023-3519 – Citrix NetScaler ADC/Gateway
- CVE-2023-22952 – SugarCRM
- CVE-2021-44228 – Apache Log4j
- CVE-2023-34362 – MOVEit
- CVE-2020-14882 – Oracle WebLogic

*2024 Incident Response Report: PaloAlto Networks Unit 42*



# Call for Action

- Protect user identities
  - Effective account management, including vendors, appropriate authentication; **MFA, PAM, RBA**
- Implement effective vulnerability management; **VM as a service**
- Implement effective processes to address vendor alerts, sector alerts, and gov agencies notices; **SOC, vCISO**

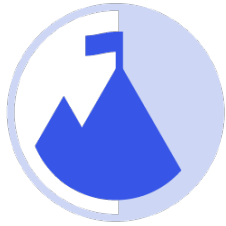


# Third-Party Risk Update

Andrew Mahler



# Third-Party Risk On the Enforcement Map



## Offices/Agencies/Entities

- HHS OCR
- FTC
- Executive Orders
- Federal legislation
- State Attorneys General
- State legislation
- Plaintiffs' Bar



## Enforcement Actions (2023)

- Use of pixels and other tracking tools on website (HHS/NY)
- Failure to address known vulnerabilities, business associate agreement failure (IN)



## Recent Concerns

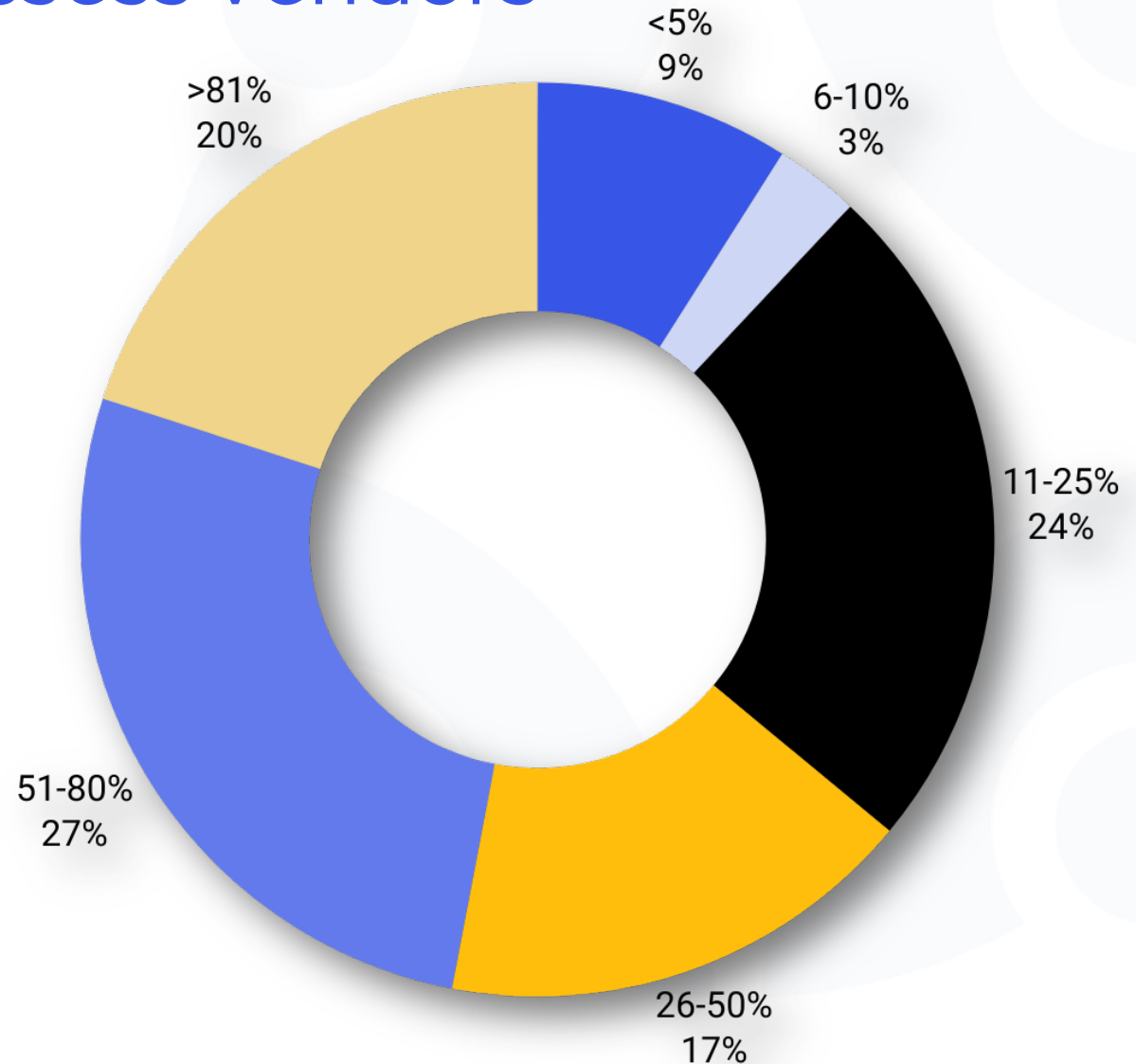
- Tracking technologies
- Artificial Intelligence
- Cyber incidents/Ransomware
- Business Associate Agreements
- Patient safety

# Third-Party Risks and OCR

- "In OCR's breach reports, over 134 million individuals have been affected by large breaches in 2023, whereas 55 million were affected in 2022. OCR recommends that health care providers, health plans, clearinghouses, and business associates...implement safeguards to mitigate or prevent cyber threats. These include:
  - *Reviewing all vendor and contractor relationships to ensure business associate agreements are in place as appropriate and address breach/security incident reporting obligations.* – February 6, 2024
- **What about paper records?**
  - The largest reported improper disposal incident in 2022 resulted from a business associate who improperly disposed of paper medical records by throwing them away in a dumpster. This breach affected approximately 7,500 individuals. Most improper disposal breaches involved disposing of paper records containing PHI in trash bins rather than authorized shred bins or another secure disposal method.

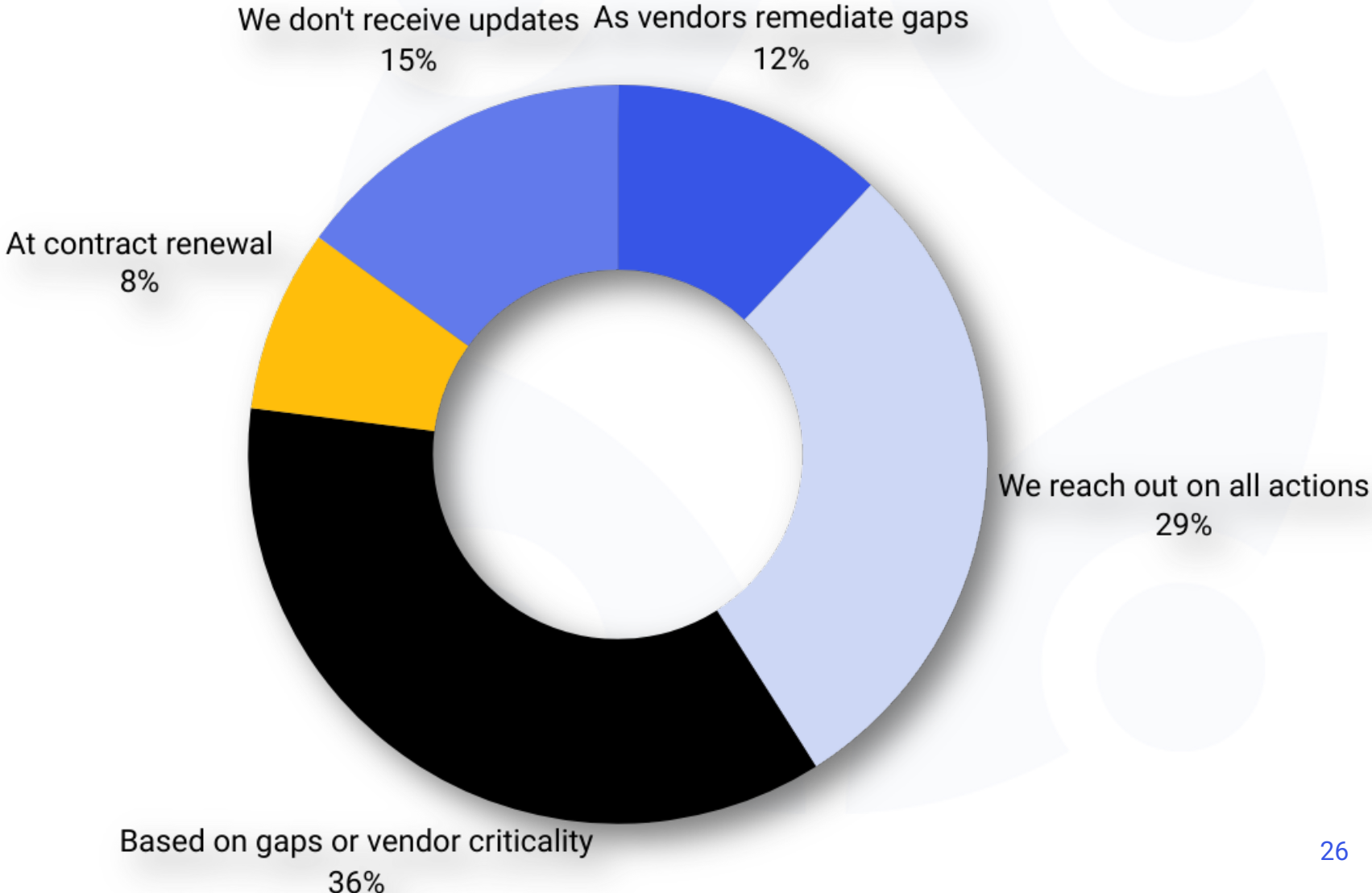
# There's WIDE variation in how consistently hospitals and covered entities assess vendors

Health 3PT asked, "What percentage of your vendor population does your organization assess"?

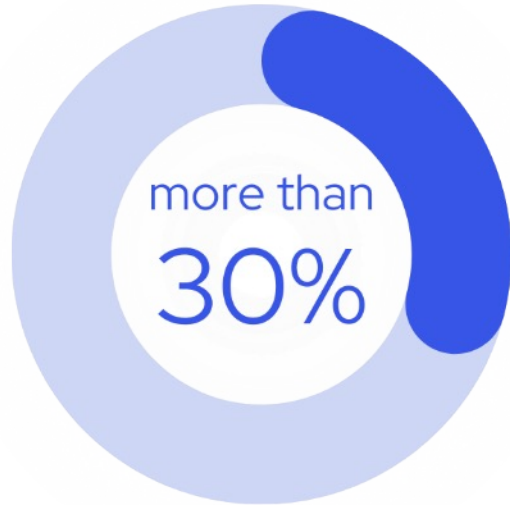




# There's also variation in how covered entities are updated on vendor remediation



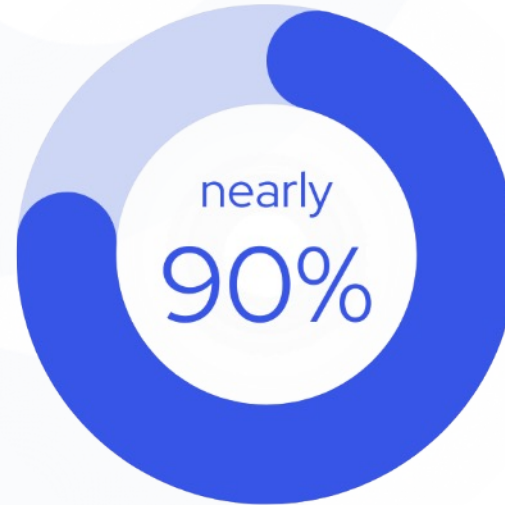
# Trends from the Clearwater Database



vendors ranked  
high risk



of vendors lacked  
basic compliance  
effort



No SOC Type 2 or  
HITRUST  
certification



A small but growing  
number of clients  
include pixel tracking  
or AI risks in their  
questionnaires.

# Third-Party Risk Management Shortcomings in Healthcare

1. No overarching methodology for risk-tiering vendors
2. Over-reliance on verbose contract terms
3. Extensive and inconsistent questionnaires that try to identify or evaluate control weaknesses
4. Limited and inconsistent validation of information collected
5. Limited follow-up and resolution of identified gaps
6. Point-in-time assessments that are rarely updated
7. Limited organization-wide insight into vendor security risk

# Practices to Consider

1. Concise contract language tying financial terms to a vendor's transparency, assurance, and collaboration on security matters
2. Risk tiering strategy that drives frequency of reviews, extent of due diligence, and urgency of remediation
3. Appropriate, reliable, and consistent assurances about the vendors' security capabilities
4. Follow-up through to closure of identified gaps and corrective action plans
5. Recurring updates of assurance of the vendors' security capabilities
6. Metrics and reporting on organization-wide vendor risks



We are here to help.

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

# Upcoming Events



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

Healthcare – Secure, Compliant, Resilient

[www.ClearwaterSecurity.com](http://www.ClearwaterSecurity.com)

800.704.3394

LinkedIn | [linkedin.com/company/clearwater-security-llc/](https://www.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.