Monthly Cyber Briefing

May 2024

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 & Speakers

- Cyber update
- Disaster Recovery and Business Continuity Planning

Steve Cagle

CEO
Clearwater

Angie Santiago

Manager, Consulting Services – Resiliency Solutions
Clearwater

Tom Joyce

vCISO, Technical Security Services
Clearwater

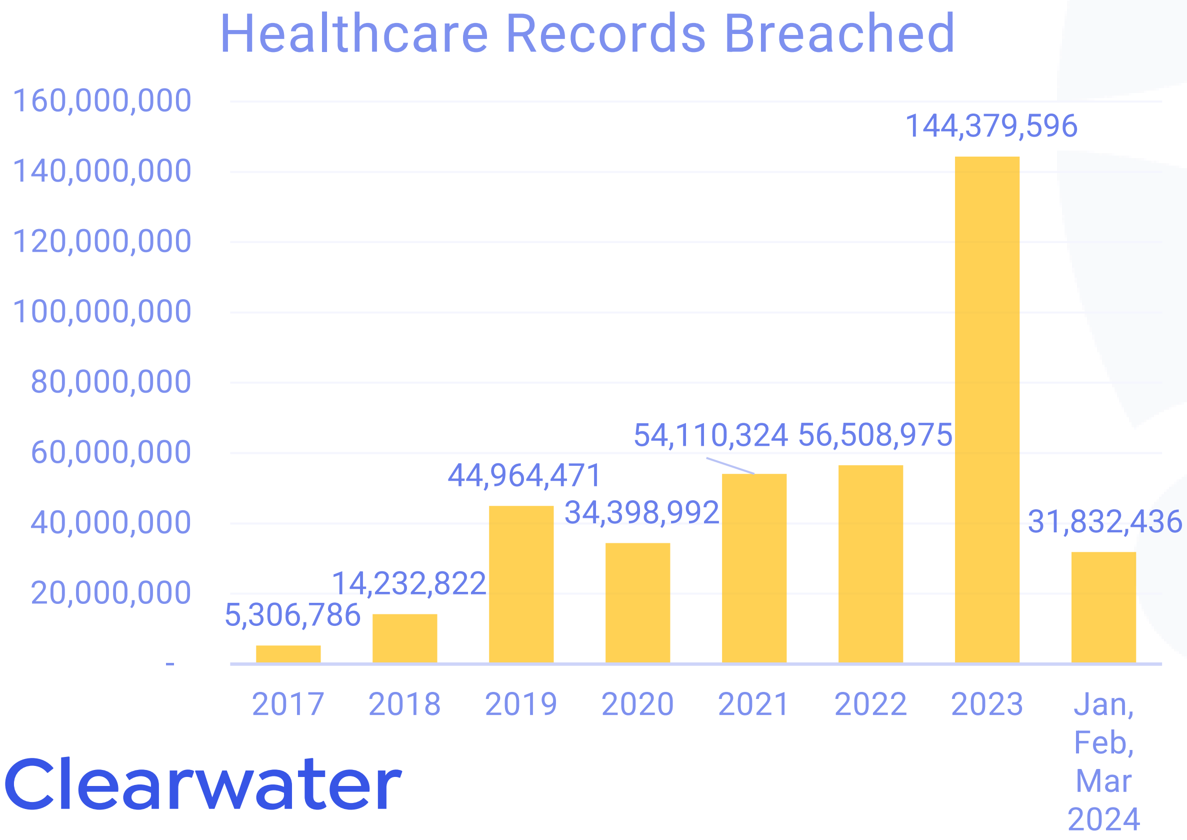
Cyber Update

Steve Cagle

Clearwater

Breach Reports via OCR Breach Portal[1]

- 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



Notable in March 2024 breach data

- About 31.8 million records (249 breaches) reported Jan – April
- Kaiser Permanente reported Unauthorized Use of 13.4M records, related to online tracking technologies
- 79% of breaches related to Hacking/IT Incident
- 57% of breached records due to Hacking/IT Incident
- If excluding Kaiser breach, 98% of breached records due to Hacking/IT Incident

[1] *HHS Breach Portal (data for 2023 pulled March 21, data for 2024 pulled April 25, 2024).*

[2] *Refer to March Cyber Briefing for top breaches of 2025*

Change Healthcare Cyber Attack Updates

United Healthcare Reports Losses

UnitedHealth reported losses already of $870M and projecting $1.6B in total losses.

Double Extortion

Notchy partners with RansomHub; leaks data and threatens further leaks if deal not reached.

Ransom Paid

UnitedHealth says they made a ransom payment. UnitedHealth was removed from RansomHub victim website.

MFA Not Enabled

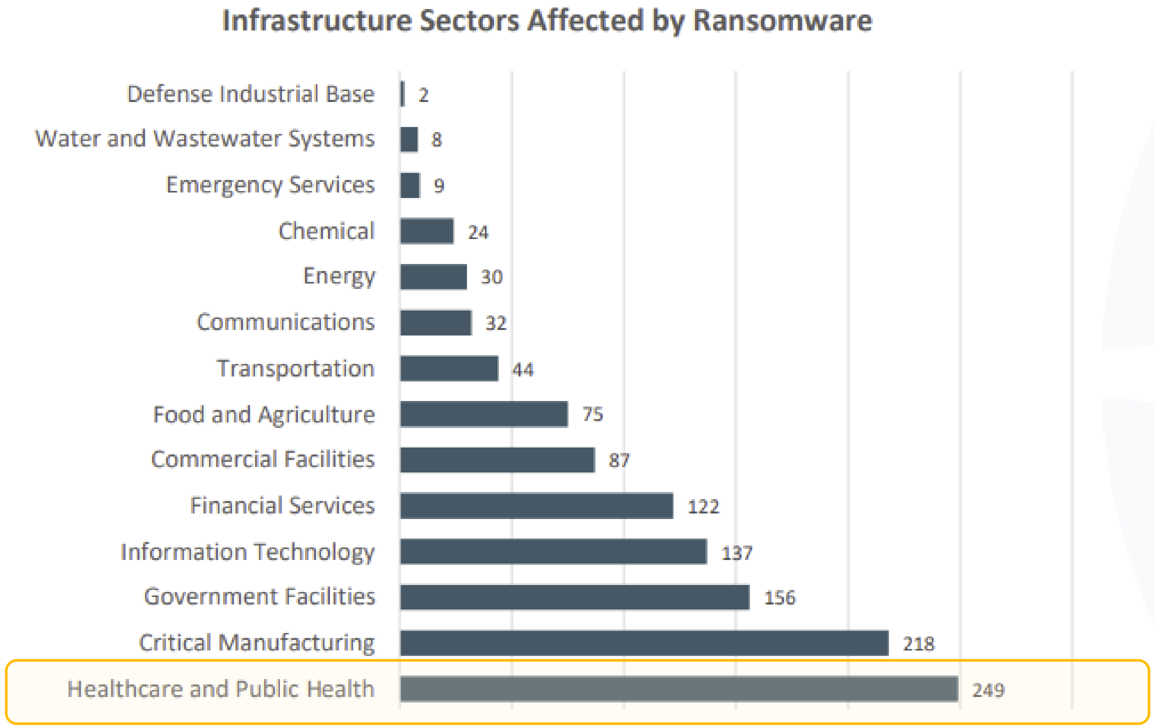
WSJ reported that the system that was breached did NOT have MFA enabled. Confirmed by CEO in Congressional testimony 5/1.

Still Recovering

UnitedHealth states medical claims flowing at “normal” levels and payment processing is at 86% of previous levels.

Clearwater

Ransomware Threat Continues to Increase



Infrastructure Sectors Affected by Ransomware

- 95% increase in Ransomware in 2023[1]
- 13% Increase in Insurance Claims – increase primarily driven by ransomware 2023[2]
- Healthcare is the most targeted critical infrastructure industry by ransomware gangs[3]
- Total losses from internet crime increased in the U.S. by 22% in 2023 to $12.5 Billion[3]
- 20% increase in reported victims in Q1 2024 vs Q1 2023[4]

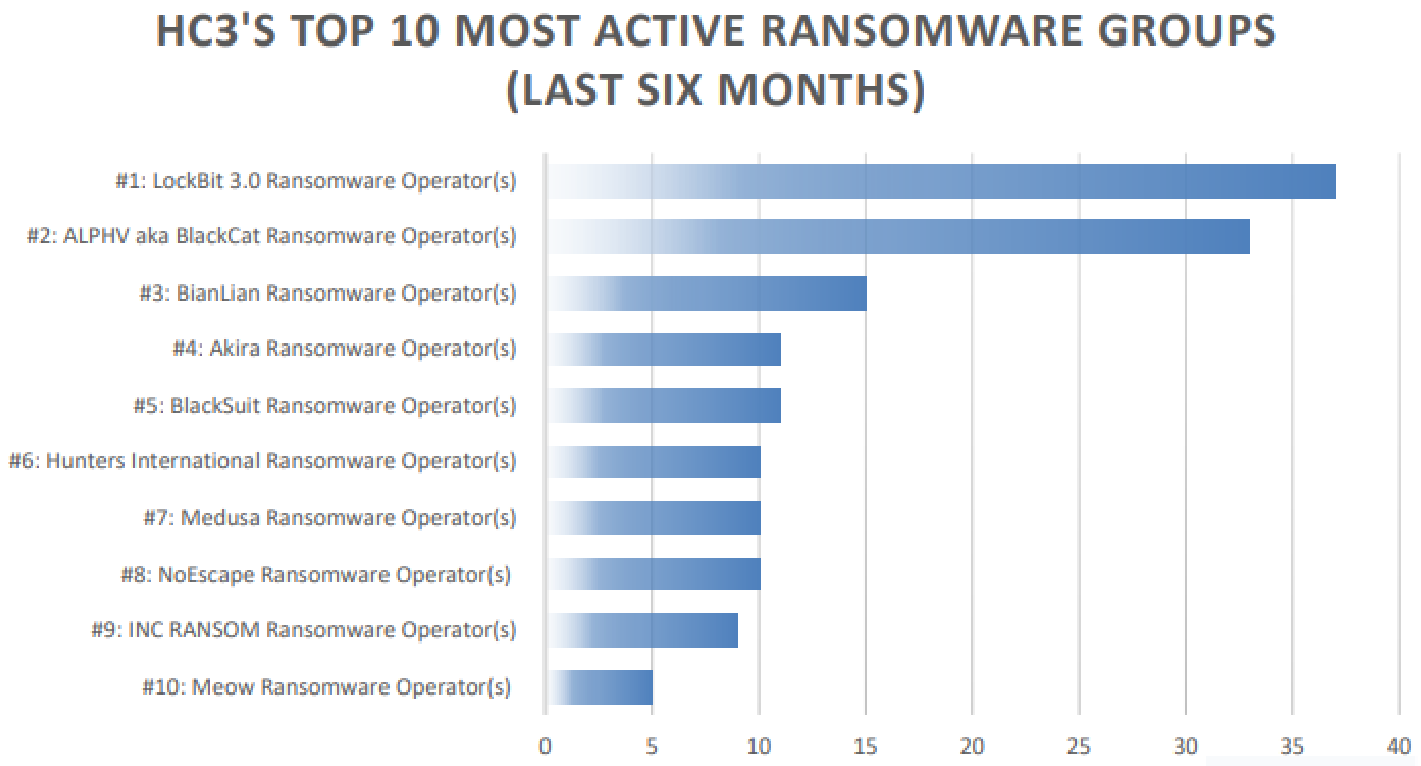
[1] *At Least 141 Were Hospitals Directly Affected by Ransomware Attacks in 2023 (hipaajournal.com)*

[2] *Ransomware triggers cyberinsurance claims increase | SC Media (scmagazine.com)*

[3] *2023 FBI Internet Crime Report.pdf*

[4] *GuidePoint Security Q1 2024 Ransomware Report*

Ransomware Actors Targeting Healthcare



HC3'S TOP 10 MOST ACTIVE RANSOMWARE GROUPS (LAST SIX MONTHS)

As of mid-March 2024, in the last six months HC3 has tracked 530 cyber attacks against the U.S. HPH, and of those attacks, nearly half were ransomware related.

202404051700_HC3's Top 10 Most Active Ransomware Groups Analyst Note_TLPCLEAR (hhs.gov)

Re-Cap of Notable Ransomware Attacks By Threat Actors Targeting HC - Last 6 Months

Ann & Robert H. Lurie Children's Hospital of Chicago®

January 2024

Bucks County

January 2024

Petersen Health Care

October 2023

CHANGE HEALTHCARE

February 2024

LMH LINDSAY MUNICIPAL HOSPITAL

March 2024

capitalhealth

November 2023

SAINT ANTHONY HOSPITAL

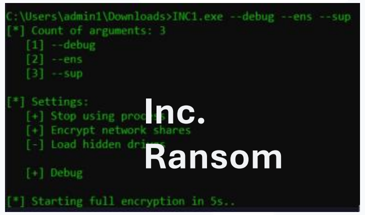
December 2023

Fred Hutch Cancer Center

December 2023

LIBERTY HOSPITAL

December 2023



```
C:\Users\admin1\Downloads>INC1.exe --debug --ens --sup
[*] Count of arguments: 3
  [1] --debug
  [2] --ens
  [3] --sup

[*] Settings:
  [+] Stop using proc
  [+] Encrypt network shares
  [-] Load hidden dri

  [+] Debug

[*] Starting full encryption in 5s..
```

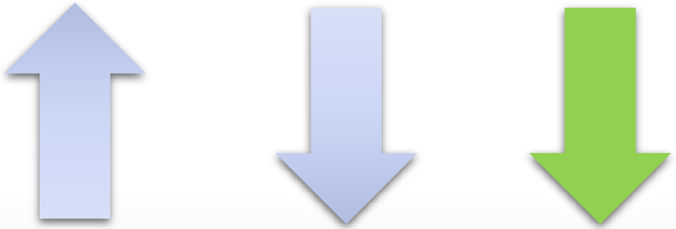
octapharma plasma®

April 2024

No Surprises with TTPs

- Threat actors going after organizations with financial motives and multiple options of extortion
- The individual continues to be the target of the adversary to steal credentials and exploit **vulnerabilities in third-party services**

Trends

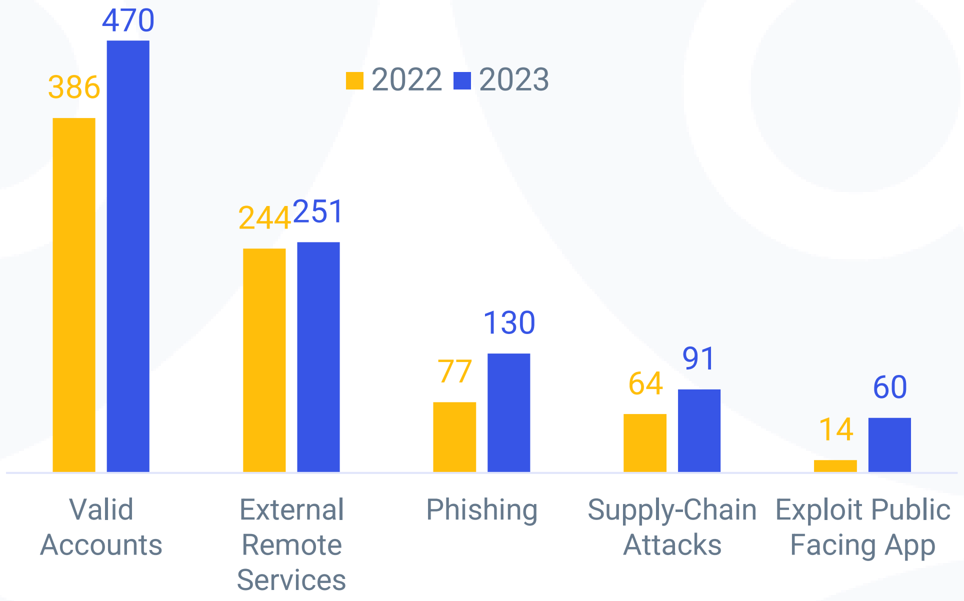


# of disclosed vulnerabilities

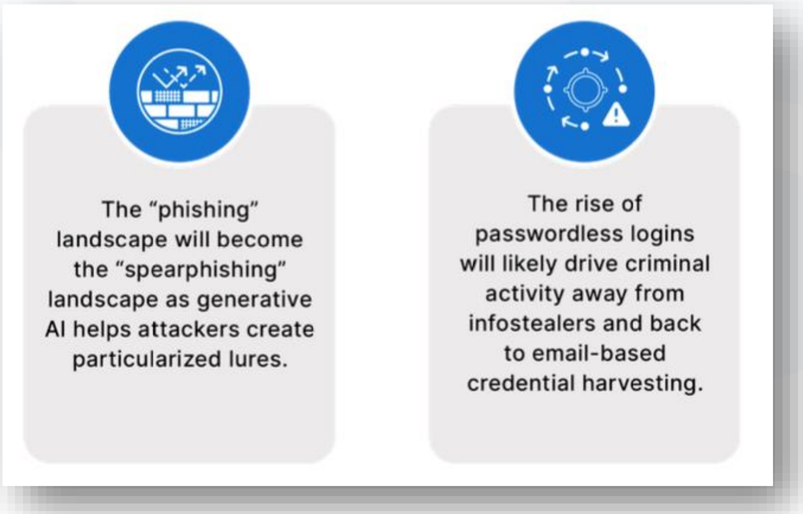
threat actor dwell time

time to address known vulnerabilities

Top 5 TTPs used to gain initial access in validated Cyberattacked (Source Recorded Future)



Recorded Future 2024 Predictions



The "phishing" landscape will become the "spearphishing" 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

Addressing TTPs of Known Threat Actors

Trend	Capabilities	Potential Actions
Zero Days, Rate of vulnerabilities	On going vulnerability management Rapid remediation of critical and high vulnerabilities Monitor and implement vendor and sector alerts	Leverage a continuous vulnerability management as a service
Exploitation where there is inconsistencies in controls	Program for Continuous Risk Analysis and Risk Response	Inventory System – Perform Asset-based Risk Analysis
Exploitation of users	Protect user identities, restrict access	Dial-up Security Awareness Training MFA, PAM, RBA
Sophistication of attacks + Growing attack surface	Identify all Information Systems Penetration Testing Security Controls Validation	Asset cataloguing Outsourced Technical Testing program vCISO + 405(d) HICP or NIST Adoption
Third Party Risk	Assess high risk vendors with more rigor and require more robust security	Leverage Vendor risk management as a service
Dwell time decrease -> Ransomware Deployment -> Exfiltration	Rapidly detect and response to compromise – orchestrate log, EDR, vulnerability data, 24/7 monitoring Business Impact Analysis IRPs, DRP, BCPs	Managed Detection & Response Services Assess and remediate resiliency program Exercise Incident response plans

Relevant Threat Indicators & Resources

- Recent HC3 Alerts
  - Palo Alto Networks Firewalls
  - Social Engineering Attacks Targeting IT Help Desks
  - Credential Harvesting
- Threat Actor TTPs & ICs Resources
  - HC3 alert on LockBit Exploiting Citrix Bleed 11/23/24
  - CISA advisory on BianLian 5/16/23
  - HC3 alert on Rhysida 8/4/23
  - CISA advisory on Rhysida Ransomware 11/15/23
  - HC3 alert on Akira on 9/12/23
  - HC3 alert on Akira on 2/7/24
  - CISA alert on Akira 4/18/24
  - HC3 analyst note on BlackSuit Ransomware on 11/6/23
  - CISA advisory on Royal (BlackSuit) 11/13/23
  - CISA advisory on BlackCat/ALPHV updated 2/27/24

Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert
April 18, 2024 TLP:CLEAR Report: 202404181500

Update: Palo Alto Networks Firewalls (CVE-2024-3400)

Executive Summary
On April 12, 2024, Palo Alto Networks issued a warning about CVE-2024-3400, a zero-day command
injection vulnerability found in its firewalls operating
both GlobalProtect gateway and device telemetry ena
attacks observed against this vulnerability since its re
disabling device telemetry would work as an effective
states that device telemetry does not need to be enal
were also released starting on April 14, 2024. HC3 st
updated security advisory and apply any mitigations t
Healthcare and Public Health (HPH) sector.

Report
Palo Alto's updated security advisory, released on Apr
increasing number of attacks targeting CVE-2024-34
Reports from Unit 42 show that threat actors are usin
the access gained to move through target organizatio
show that approximately 156,000 instances have be
under the name Operation MidnightEclipse. For furthe
including indicators of compromise, please refer to th
from Volexity can be found here. For the most up-to-d
Palo Alto's Security Advisory.

Current advisories from Palo Alto Networks report tha
11.0, and PAN-OS 11.1 firewalls configured with Glob
Importantly, this issue does not impact cloud firewalls
Access.

Patches, Mitigations, and Workarounds
According to Palo Alto: "We strongly advise customers
to protect their devices even when workarounds and
PAN-OS 10.2.9-h1, PAN-OS 11.0.4-h1, PAN-OS 11.1.2
upgrade to these versions will be fully protected. In ad
for customers, additional hotfixes are being made ava
maintenance releases and will also be made availabl
wait for these hotfixes."

PAN-OS 10.2:
- 10.2.9-h1 (Released 4/14/24)
- 10.2.8-h3 (Released 4/15/24)
- 10.2.7-h8 (Released 4/15/24)
- 10.2.6-h3 (Released 4/16/24)
- 10.2.5-h6 (Released 4/16/24)

[TLP:CLEAR, ID#20240
U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3) www.HHS.GOV/

Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert
April 3, 2024 TLP:CLEAR Report: 202404031000

Social Engineering Attacks Targeting IT Help Desks in the Health Sector

Executive Summary
HC3 has recently observed threat actors employing advanced social engineering tactics to target IT help
desks in the health sector and gain initial access to target organizations. In general, threat actors continue
to evolve their tactics, techniques, and procedures (TTPs) to achieve their goals. HC3 recommends various
mitigations outlined in this alert, whic
for increased security for identity verif

Report
Social engineering is being used acro
unauthorized access to systems. Thre
to target an organization's IT help des
claiming to be an employee in a finan
threat actor is able to provide the req
four digits of the target employee's so
other demographic details. These det
publicly available information sources
phone was broken, and therefore cou
successfully convinced the IT help des
access to corporate resources.

After gaining access, the threat actor
where they then submitted a form to
to employee email accounts, they sen
attacker-controlled U.S. bank account
malicious campaign, the threat actor
organization and created an account

Analysis
There was a recent high profile incide
organization in the hospitality and ent
Scattered Spider (also known as UNC
deployment of ALPHV (also known as
incident in the health sector.

While these recent campaigns in the
leverage spearphishing voice techniq
the threat actors' end goals. Spearphi
different from other forms of spearph
access to systems through a phone c
involves social engineering technique
creating a sense of urgency or alarm

It is important to note that threat acto
social engineer targets, making remo

U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center

Office of Information Security
Securing One 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

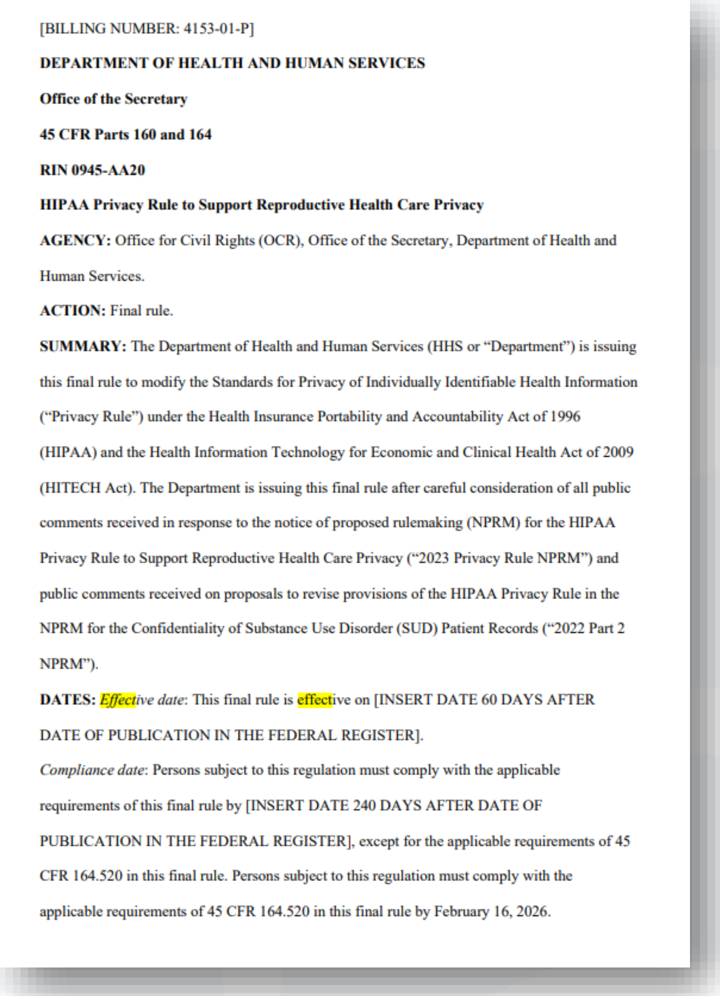
[TLP:CLEAR, ID#202403181500, Page 1 of 3]
U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3) www.HHS.GOV/HC3

Regulatory Updates

Steve Cagle

New Rule to Support Reproductive Health Care Privacy Under HIPAA

- Prohibits the use or disclosure of PHI when it is sought to investigate or impose liability for lawful reproductive healthcare care
- CEs and BAs must obtain a signed attestation that requests for PHI related to reproductive health care are not for these prohibited purposes
- Requires regulated health care providers, health plans, and clearinghouses to modify their Notice of Privacy Practices to support reproductive health care privacy



[BILLING NUMBER: 4153-01-P]

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN 0945-AA20

HIPAA Privacy Rule to Support Reproductive Health Care Privacy

AGENCY: Office for Civil Rights (OCR), Office of the Secretary, Department of Health and Human Services.

ACTION: Final rule.

SUMMARY: The Department of Health and Human Services (HHS or "Department") is issuing this final rule to modify the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The Department is issuing this final rule after careful consideration of all public comments received in response to the notice of proposed rulemaking (NPRM) for the HIPAA Privacy Rule to Support Reproductive Health Care Privacy ("2023 Privacy Rule NPRM") and public comments received on proposals to revise provisions of the HIPAA Privacy Rule in the NPRM for the Confidentiality of Substance Use Disorder (SUD) Patient Records ("2022 Part 2 NPRM").

DATES: *Effective date*: This final rule is effective on [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

Compliance date: Persons subject to this regulation must comply with the applicable requirements of this final rule by [INSERT DATE 240 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], except for the applicable requirements of 45 CFR 164.520 in this final rule. Persons subject to this regulation must comply with the applicable requirements of 45 CFR 164.520 in this final rule by February 16, 2026.

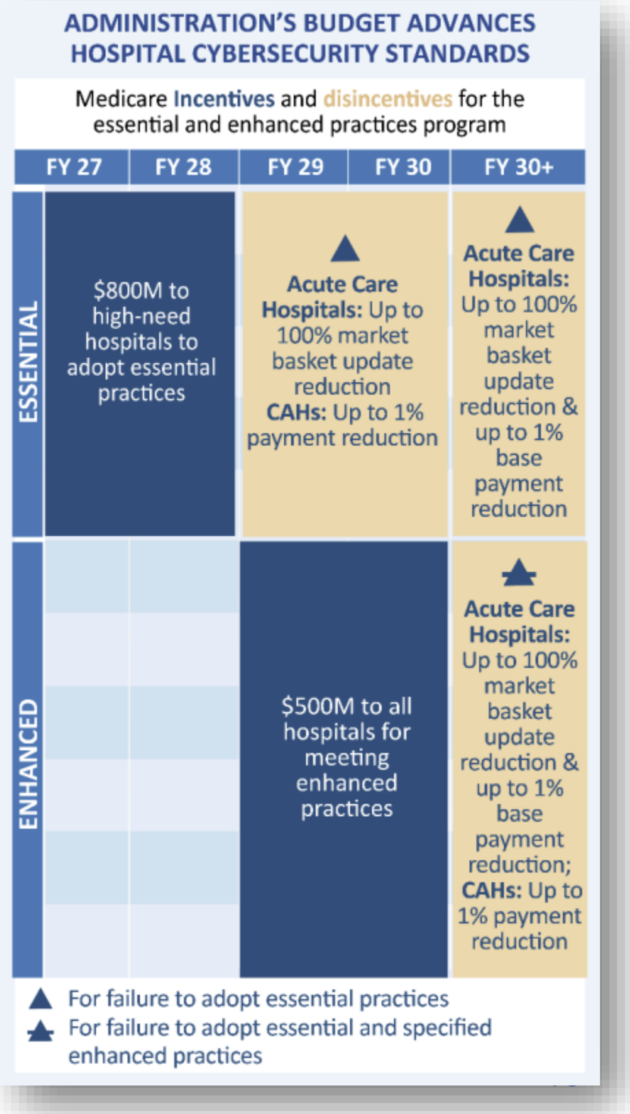
HHS 2025 Budget Proposal Calls for More Funding - and More Penalties – Related to CPGs For Hospitals

- 2025 Biden administration/HHS budget proposal for cybersecurity based on Healthcare Cybersecurity Performance Goals
  - $800 million for high need (2,000) hospitals for essential cybersecurity practices FY 2027 - 2028
  - $500 million incentive program for enhanced cybersecurity practices for all hospitals FY 2029 - 2031
  - Funding through Promoting Interoperability
  - Penalties begin FY 2029 and increase in size in FY 2031
  - By 2031 both Essential and Enhanced required
- Concerns with this program
  - Slow drip of funding over 10 years
  - No incentives in 2025 or 2026
  - Only applies to hospitals

Fiscal Year 2025

Budget in Brief

U.S. Department of Health & Human Services
HHS.GOV



ADMINISTRATION'S BUDGET ADVANCES HOSPITAL CYBERSECURITY STANDARDS

Medicare Incentives and disincentives for the essential and enhanced practices program

	FY 27	FY 28	FY 29	FY 30	FY 30+
ESSENTIAL	$800M to high-need hospitals to adopt essential practices		▲ **Acute Care Hospitals:** Up to 100% market basket update reduction **CAHs:** Up to 1% payment reduction		▲ **Acute Care Hospitals:** Up to 100% market basket update reduction & up to 1% base payment reduction
ENHANCED			$500M to all hospitals for meeting enhanced practices		⏫ **Acute Care Hospitals:** Up to 100% market basket update reduction & up to 1% base payment reduction; **CAHs:** Up to 1% payment reduction

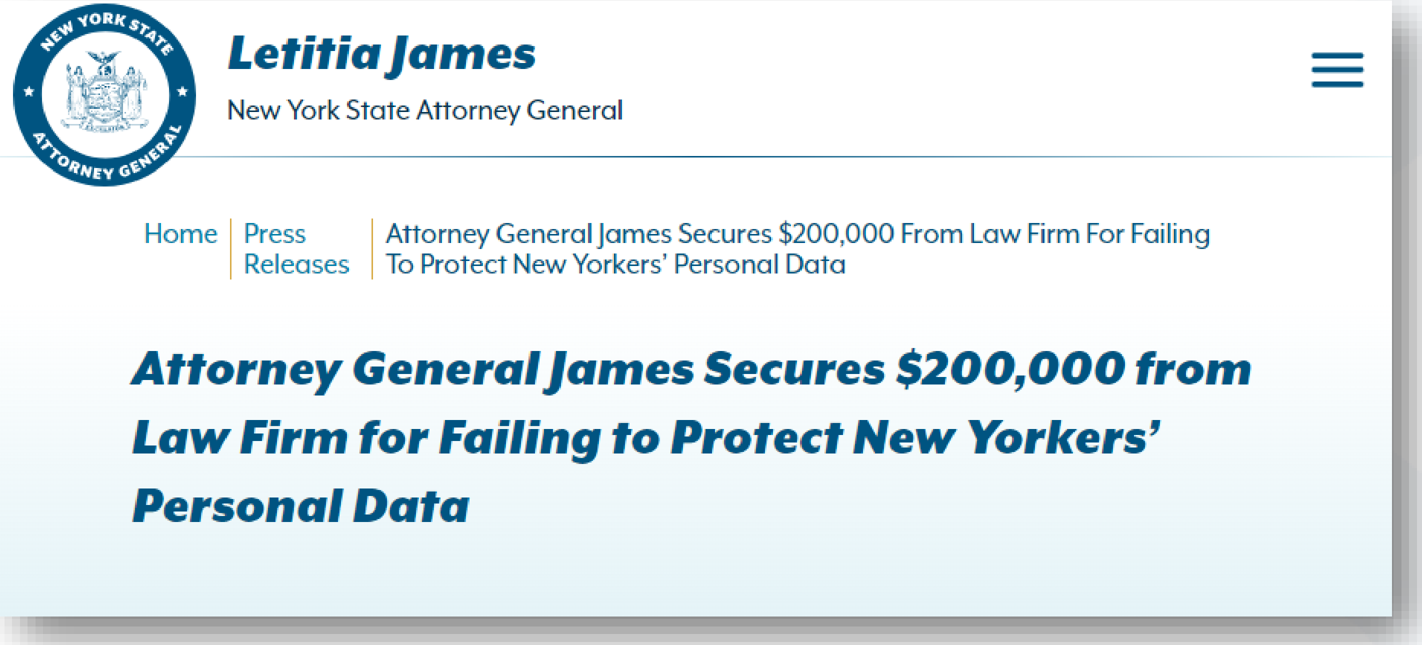
▲ For failure to adopt essential practices

⏫ For failure to adopt essential and specified enhanced practices

Clearwater

HHS FY 2025-budget-in-brief.pdf (hhs.gov)

State Attorney General Actions



Letitia James

New York State Attorney General

Home | Press Releases | Attorney General James Secures $200,000 From Law Firm For Failing To Protect New Yorkers' Personal Data

Attorney General James Secures $200,000 from Law Firm for Failing to Protect New Yorkers' Personal Data

- Failure to assess and remediate known vulnerabilities
- Suffered LockBit ransomware attack
- Failed to timely notify 61,438 New York residents of breach
- 17 total counts of HIPAA and state law security violations

Other Updates (Some Covered in Previous Cyber Briefings)

- CIRCIA Final Rule was published on 3/27/2024, 60-day comment period starting 4/4/24, and will go into effect within 18 months from publication
- HHS to restart Auditing program later this year. Also seeking increase in penalties for HIPAA violations
- HHS Updated Guidance on Tracking Technologies
- FTC Prohibits Monument (Alcohol Addiction Firm) from Sharing Consumer Data. Also fines $2.5 Civil Monetary Penalty (suspended) in fourth enforcement case related to online tracking technologies

Compliance Recommendations

1. Evaluate use of online tracking technologies
2. Complete Gap Assessments of HIPAA and State requirements
3. Ensure OCR-Quality Risk Analysis is up to date
4. Make updates to policies and procedures
5. Assess your implementation of 405(d) HICP

Disaster Recovery and Business Continuity Planning

Angie Santiago

Tom Joyce

Clearwater

Angie M. Santiago, MA, CBCP

- Disaster Management Systems Methodology Designer & Educator
- Healthcare Disaster Operations & Long-Term Recovery
- Emergency Management, Business Continuity, Disaster Recovery
- Conflict Management & Resolution
- 100 plus programs, 200 plus exercises, 60 plus major disaster declarations
- Partnership for Inclusive Disaster Strategies
- Resilient Nation Partnership Network
- CISA 405(d) Task Force
- Institute for Diversity in Emergency Management
- InfraGard
- Information System Security Association
- Women in Cybersecurity

Tom Joyce, CISSP, CHPCP, CCFSP, MPM

- Experienced cybersecurity leader in multiple industries: healthcare, finance, manufacturing, higher education
- Former CISO – Mountain Health Network (now Marshall University Health)
- Member – InfraGard, ISSA, ISC2, DRI
- BS Applied Mathematics – Scientific Computing & Engineering Systems, Carnegie Mellon University

How ready is your organization?

Life & Safety
Emergency
Mgmt.
Community
Preparedness

Internal /
External
Communications

Continuity of
Care &
Operations

Medical Surge
Mass Casualty
Public Health

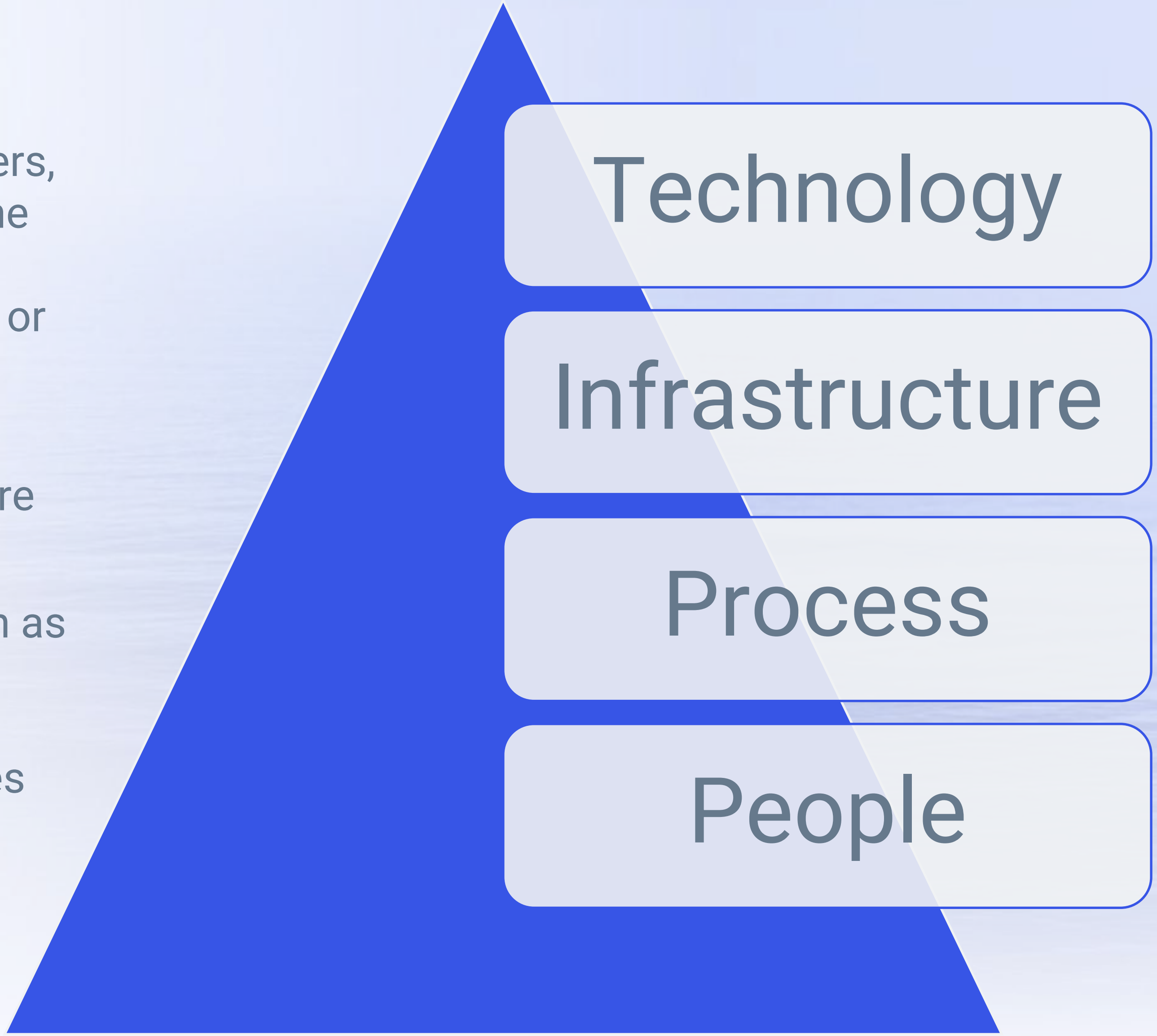
Information
Technology &
Cybersecurity

Infrastructure
Facilities

Technology Disruption

Foundational Priorities

- **People**: Patients, providers, staff, students, partners, and volunteers are the most important asset to the delivery of safe patient care, operations and administration of the practice, healthcare system or research activities.
- **Process**: Critical clinical, business, and administrative functions provide direct patient care and ensure the viability of the healthcare system.
- **Infrastructure:** Critical unseen infrastructure such as secure and resilient facilities, HVAC, telecommunications, utilities, water, sewage, sterilization, oxygen, telecommunications provides the capacity to deliver safe quality healthcare.
- **Technology**: Availability and resiliency of the technologies which support critical services.



Clearwater

Q&A

We are here to help.

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

Upcoming Events

#HCPE2024
HCPE
20TH ANNUAL
HEALTHCARE PRIVATE EQUITY AND FINANCE CONFERENCE
May 8-9, 2024 | The Ritz-Carlton, Chicago
McGuireWoods
www.healthcareprivateequity.com

McGuireWoods Healthcare Privacy Equity & Finance Conference | May 8-9, 2024

A Conversation About Cybersecurity in Healthcare | May 9, 2024

HIMSS
CENTRAL & SOUTHERN OHIO CHAPTER

Central Southern Ohio HIMSS Spring Conference | May 10, 2024

Cyber Assurance in Healthcare: Insights from HITRUST and Clearwater | May 22 @ 12:00 CST

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.