Healthcare’s Cyber Briefing

November 5, 2026

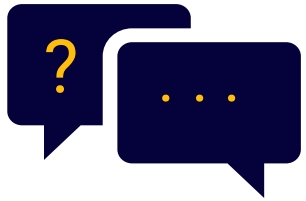
Clearwater

Meeting Logistics



Microphones

All attendees are on mute.



Questions

Type your questions in the Q&A box.



Resources

Upcoming events, slides & resources linked.



Recording

Recording will be provided after event.



Survey

Survey will prompt at the end of webinar.

©2026 Clearwater Security & Compliance LLC

HEALTHCARE'S CYBER BRIEFING

Agenda

- Critical Threat Brief
- Education Session: Preparing for Disruptions in AI-Assisted Clinical Care
- Q+A

Clearwater



Dave Bailey

VP of Consulting Solutions & Strategy



Dr. Benoit Desjardins

Professor of Radiology, University of Montreal; Chief Medical Cybersecurity Officer (CMCO) and Chief Medical Information Officer (CMIO) in Radiology, CHUM

HEALTHCARE'S CYBER BRIEFING

Healthcare Industry Threat Information

- Artificial Intelligence

Clearwater

October Showed What AI-Speed Exploitation Looks Like in Practice

1

A vulnerability tsunami

AI-assisted code auditing is surfacing architectural flaws faster than vendors can patch them. October's emergency disclosures included critical memory-safety flaws in the PHP runtime.

2

Automated, then hands-on

Attackers scripted scans and exploitation of public-facing services. Late-October intrusions paired remote code execution with privilege escalation and persistent reverse-SSH tunnels.

3

AI inside the toolchain

Forensics recovered offensive tooling wired into commercial LLM APIs and autonomous vulnerability scanners. Adversaries are embedding frontier models in command and control.

Your patch window is now your exposure window: prioritize by exploitability, not CVSS alone.

Source: Google Threat Intelligence

Agentic AI Is Now an Intrusion Tool: Storm-0940 and ARTEX

<3 hrs

from initial targeting to privileged cloud access in some cases

2,250+

Microsoft 365 tenants targeted through ConnectWise Cloud Backup app identities

~2,900/min

sign-in attempts at peak during the campaign

How the chain worked

1. Stolen application credentials from ConnectWise Cloud Backup (disclosed Oct 16)
2. ARTEX agents run reconnaissance, password spraying, and OAuth app abuse
3. Applications already granted access authenticate without an interactive sign-in
4. Attackers add credentials and identities for privileged cloud persistence

China-state-aligned actor, open-source framework. ARTEX is a multi-agent penetration-testing framework Microsoft says several actors now use. Google Threat Intelligence also saw malicious packages pushed through LiteLLM and exploitation of command-injection flaws in enterprise generative AI connectors.

Review OAuth grants and third-party app identities now: backup and MSP tools hold many keys.

Sources: Microsoft Threat Intelligence (Oct 21); The Record; Dark Reading; Google Threat Intelligence.

AI Attack Planning Reaches Industrial Systems; Hospitals Share the Grid

~90%

of 500+ simulated industrial control scenarios produced actionable AI attack plans (DOE-supported evaluation)

~2 yrs

researchers' estimate before models can independently navigate industrial environments

What Google Threat Intelligence observed

- Iranian-linked CyberAv3ngers sustained opportunistic attacks on PLCs and water utilities across multiple states.
- MITRE ATT&CK v20 (mid-October) adds techniques for AI-enabled OT compromise, prompt injection, and automated OT command execution.
- FERC audits warn that unmanaged AI tools can bridge administrative networks and protected control perimeters.

Where this touches hospitals: building management, HVAC, medical gas, generators, and the regional power and water that cloud-hosted AI tools also depend on.

Inventory OT and building systems, and any AI tool with network reach. Keep both off flat networks.

Source: Google Threat Intelligence, AI Threats to U.S. Critical Infrastructure: October 2026 Assessment.

Washington's Response: Anticipatory Defense, Voluntary Guardrails, Pending Bills

STRATEGY · OCT 26

CISA 2030: Defend, Harden, Prevail

Pivots from passive mitigation to anticipatory defense: find and remove adversary footholds before automated tooling can weaponize them. CISA plans a 60-day service review and a 180-day implementation plan.

VOLUNTARY GUIDANCE · OCT 16

NIST, NSA, and CISA: AI agent control incidents

Ten practices across five lifecycle stages: least privilege, single-use infrastructure, automatic stop of affected agent runs, and recovery from known-good baselines. A useful template for any client deploying agents.

PROPOSED · OCT 22 · NOT LAW

AI Cyber Defense Act (H.R. 10873)

Bipartisan House bill directing NIST to develop voluntary guidance against AI distillation attacks and to convene defenders. Referred to the House Science Committee.

Google Threat Intelligence also reports that an Oct 17 insider arrest at a frontier AI lab prompted a White House AI Task Force led by the Director of National Intelligence.

Expect more guidance than mandates in the near term. Clients can adopt the voluntary practices now.

Sources: CISA; NIST, NSA, and CISA joint guidance (Oct 16); Congress.gov (H.R. 10873); Google Threat Intelligence.

HEALTHCARE'S CYBER BRIEFING

Healthcare Industry Threat Information

- Disruptive Adversarial Attacks: Nation-state tradecraft, takedowns, and operational disruption

Clearwater

Federal Advisory and Industry Takedown: Pressure on Adversary Infrastructure

JOINT ADVISORY AA26-281A · OCT 8

Integrity Technology Group enables China-linked intrusions

- CISA, FBI, NSA, and partners in the UK, Australia, Canada, Japan, New Zealand, and Spain tie tooling and infrastructure to China-based Integrity Tech.
- Automated scanning, botnets, VPN infrastructure, and living off the land, paired with hands-on exploitation.
- Victims include government, manufacturing, healthcare, law enforcement, and education.

MICROSOFT + HEALTH-ISAC · OCT 15

Three cybercrime service businesses disrupted

- YAM Store, CoGUI, and Iron Man, part of a Chinese-language marketplace, were disrupted through domain seizures.
- Their services supported attacks on 75,000+ organizations in 150+ countries, including healthcare.
- More than 1 billion malicious messages and tens of millions of dollars in proceeds.

Exploited edge devices to check this week: Citrix NetScaler ADC and Gateway zero-day (CVE-2026-88779, SAML-configured systems; emergency updates Oct 5) and four SonicWall SMA 1000 vulnerabilities (hotfixes Oct 6–7), one rated CVSS 10.

Edge devices are the common thread: inventory them, patch them, and monitor for persistence.

Sources: CISA AA26-281A; AHA News (Oct 16); Health-ISAC TLP:WHITE bulletins (Oct 5–13).

When Systems Go Down: Two October Incidents Hit Patient Operations

UNM HEALTH · OCT 26

Ambulance diversion at New Mexico's only Level I trauma center

- Ambulances diverted for two hours; outpatient procedures and new intake limited.
- Critical systems back online Oct 27. UNM said end-user devices were affected but core systems and servers were not penetrated.
- A new group, Byod, claimed the attack and data theft. UNM has not confirmed.

UNIVERSITY HOSPITALS · OCT 22

Websites and MyChart offline for a week

- "Unusual activity" on servers led the system to disconnect its websites and MyChart from the internet.
- Still largely down a week later. The internal network was unaffected, so clinicians kept access to patient records.
- The cause has not been publicly confirmed.

> **Lesson:** patient-facing portals belong in your downtime plan. Separate clinical access from public-facing systems and pre-draft patient communications.

Sources: HIPAA Journal; BleepingComputer; Help Net Security; Ideastream (Oct 26–29). Attacker claims are unverified.

HEALTHCARE'S CYBER BRIEFING

Healthcare Industry Threat Information

- Ransomware: October sets a new high for leak-site postings

Clearwater

October Posted the Busiest Month of 2026: 78 Victims

78

victims in October through Oct 29; +50% vs. both Sept and Oct 2025

474

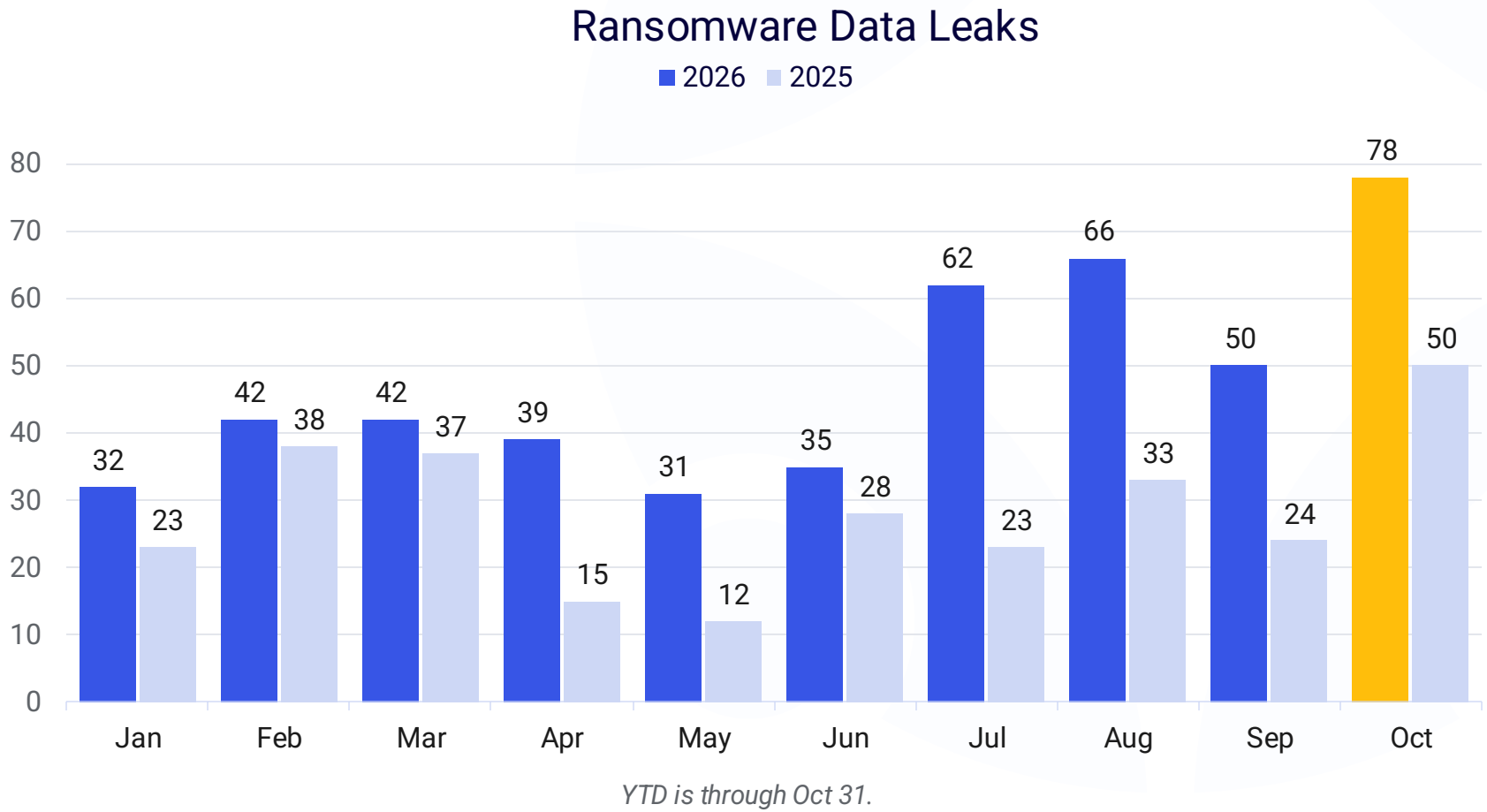
YTD victims, +69% vs. 283 in the same window of 2025

77

distinct groups YTD (58 in 2025); 30 were active in October

11.0

victims a week YTD, up from 6.5 in 2025

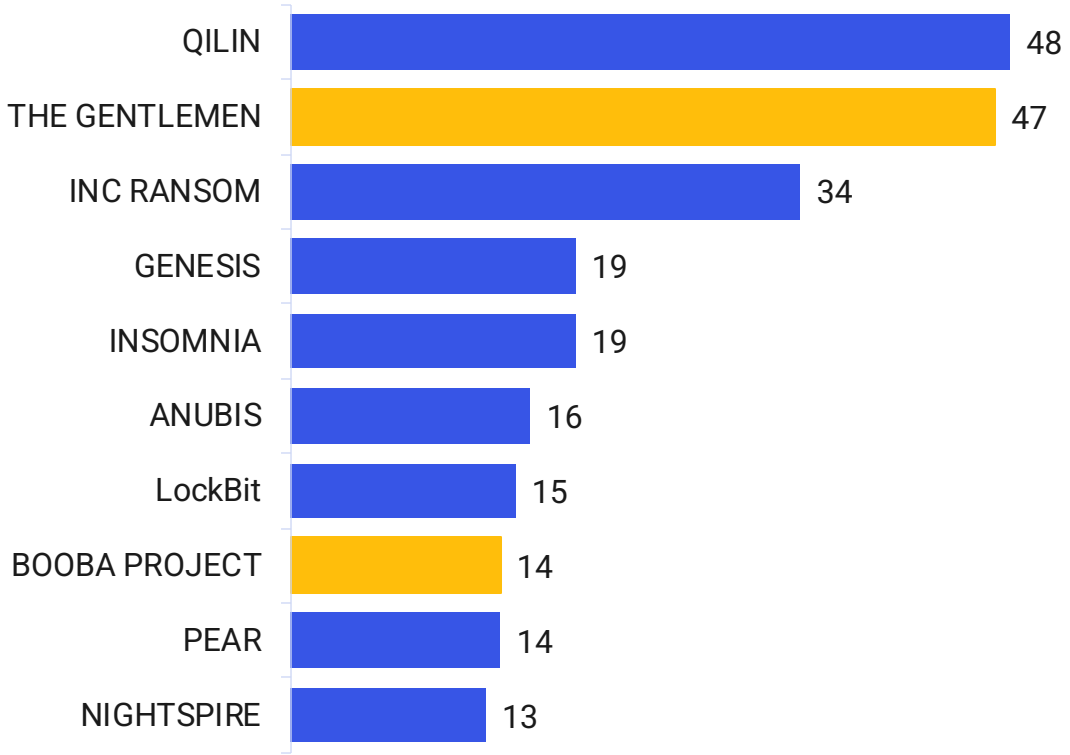


YTD is through Oct 31.

Source: Google Threat Intelligence dark-web leak-site monitoring (U.S. healthcare and pharma)

The Gentlemen Close In on Qilin YTD, While Booba Project Surges in Oct

Top 10 actors, 2026 YTD victims



October leaders

Booba Project	12
The Gentlemen	12
N0N	5
Interlock	4
Inc Ransom	4

Qilin has gone quiet in U.S. healthcare

- Qilin posted 9 victims in July, then 1, 1, and 2 in August through October.
- A suspected core member was extradited from Japan to Germany on Oct 2, but reporting says the group kept posting widely, so the arrest does not explain the lull.
- Six brands first listed in October: Kubera, Netrunner, Helix, Hyflock, Rhysida, Vypr.

Sources: Google Threat Intelligence leak-site monitoring

Threat Actor Profile: Booba Project Targets Practice Groups

14
U.S. healthcare victims claimed YTD

12
posted in October, 2 in September

10 of 14
were specialty or behavioral practices

10–200 GB
claimed per victim, all sectors

How the attack unfolds

1. **Access:** exposed RDP or admin gateways with stolen credentials
2. **Move:** WMI (T1047) and compromised local and domain accounts
3. **Steal:** stage and exfiltrate archives from high-value shares
4. **Disable:** kill security agents, delete shadow copies (T1490)
5. **Extort:** encrypt to .booba, drop booba.txt, list on a Tor leak site

What to do now

- Put RDP and admin interfaces behind a gateway with phishing-resistant MFA.
- Keep immutable, isolated backups that do not share domain credentials.
- Alert on vssadmin and wmic shadow copy deletion and unusual WMI or PowerShell.
- Watch for large outbound archive transfers from file shares.
- Reset credentials exposed in infostealer logs.

Exposed remote access plus stolen credentials is the front door. Close it first.

Sources: Booba Project campaign summary (VirusTotal collections); Google Threat Intelligence leak-site monitoring via Clearwater dashboard. Leak-site claims are actor-asserted.

Specialty Practices Remain the Top Target Across Leading Actors

Threat actor	Hospital	Specialty Practice	Behav. Health	Dental	Diag-nostic	Senior & Home	Pharma	Med Dev / Supply	Svcs / Tech	Re-search	Health Plan	Well-ness	Other*	Total
QILIN	2	12	6	9	3	5	1	2	4			2	3	49
THE GENTLEMEN	7	18	1	7	2	3	1	1	2	2	1	1	1	47
INC RANSOM	2	13	1	2	3	4	4	1	1	1		2		34
GENESIS	1	10		1	1	1	1		1	1	1		2	20
INSOMNIA		12	1		1	3		1				1		19
ANUBIS	2	5	1	2		3		3						16
LockBit	1	4	1	3	1	1		1			1	1	1	15
BOOBA PROJECT		9	1			1		1				1	1	14
PEAR		9	1	2			1		1					14
NIGHTSPIRE	1	2	1	2		2		1		4				13
CHAOS		3		1	1		3	1	1	1	1			12
STORM	3	2	1		1	1	1	1	2					12
AKIRA				3	2		1	1	1	1		1	1	11
ALL ACTORS	39	152	20	59	26	39	23	38	28	19	7	13	14	477

VICTIMS 1 | 2–3 | 4–5 | 6–9 | 10+

Top 13 actors by YTD volume; ALL ACTORS covers all 77 groups (477 victims).

HEALTHCARE'S CYBER BRIEFING

Healthcare Industry Threat Information

- Breach Portal and Regulatory Update – OCR data through Oct 8 reporting, enforcement, HTI-5, and AI Clinical Reslience

Clearwater

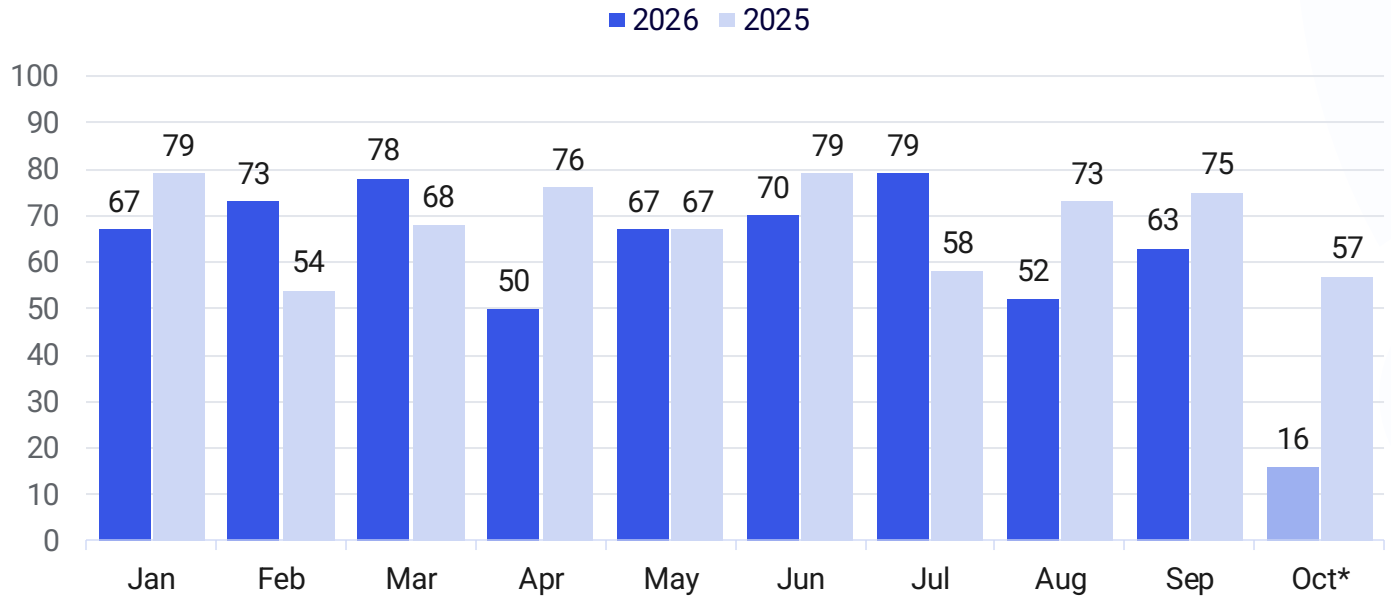
2026 HIPAA Breach Report: 615 Reported Breaches Through Oct 8 Reporting

615
reported breaches, Jan 1–Oct 8

87.7M
individuals affected

16
mega-breaches (≥1M) = 80% of individuals

86%
hacking/IT incidents (527 of 615)



**October 2026 is partial (through Oct 8). Counts by OCR portal receipt month.*

Largest October filings so far

- **iRhythm Technologies: 8.18M** (Oct 3), 96% of October individuals to date. Health-ISAC named iRhythm in its July ShinyHunters alert.
- **Denver Health Medical Plan: 238K** with a business associate involved.
- **Cognitive Health Technologies: 49K** (business associate).
- OCR's portal posts breaches weeks after filing. Jan–Sep has been restated to 599 breaches and 79.1M individuals (555 and 76.5M in October's briefing), so October is incomplete.

Source: HHS OCR Breach Portal, active and archive exports through Oct 8, 2026, via Clearwater 2026 HIPAA Breach Landscape Dashboard. Portal data reflects reported breaches, not incidents.

16 Mega-Breaches Account for 80% of the 87.7M Individuals Affected

Entity	Filed	Entity type	Individuals
DentaQuest, LLC	Jul 16	Health plan	15.00M
Aesto, LLC	Jul 31	Business associate	9.54M
iRhythm Technologies, Inc.	**Oct 3**	**Provider**	8.18M
Lumexa Imaging	May 15	Provider	5.83M
AdaptHealth, LLC	Aug 14	Provider	4.12M
Unlimited Technology Systems, LLC	Jul 21	Business associate	3.80M
CareCloud, Inc.	Jul 24	Business associate	3.76M
TriZetto Provider Solutions	Feb 6	Business associate	3.43M
QualDerm Partners, LLC	Feb 22	Provider	2.95M
Baylor Genetics	Aug 14	Provider	2.81M
Nacogdoches Memorial Hospital	Mar 30	Provider	2.51M
Navia Benefit Solutions, Inc.	Mar 18	Business associate	2.15M
Insightin Health, Inc.	Jan 16	Business associate	1.95M
New York City Health and Hospitals Corporation	Mar 24	Provider	1.80M
Xsolis, Inc.	Jun 5	Business associate	1.40M
MCBS, LLC	Jun 26	Business associate	1.26M

Source: HHS OCR Breach Portal through Oct 8, 2026. Entity type as reported to OCR.

What stands out

- **Business associates: 8 of 16.** BAs filed 36% of all individuals affected YTD.
- **All 16 were hacking/IT incidents.** None was a lost laptop or misdirected mailing.
- **July alone** brought 4 mega-breaches, including DentaQuest (15M) and Aesto (9.5M).
- **Compliance takeaway:** vendor access, logging, and notification timing belong in your BAAs and your risk analysis.

OCR Enforcement: Lehigh Valley Health Network Pays $800K, 2026's Largest Action

Date	Respondent	Type	Penalty
Feb 19	Top of the World Ranch Treatment Center	Provider	$103K
Mar 5	MMG Fusion, LLC	Business associate	$10K
Apr 23	Regional Women's Health Group (Axia)	Provider	$320K
Apr 23	Assured Imaging Affiliated Covered Entities	Provider	$375K
Apr 23	Consociate Health	Business associate	$225K
Apr 23	Star Group Health Benefits Plan	Health plan	$245K
Jun 18	Spencer Gifts Health Plan	Health plan	$450K
Jul 29	OSF Healthcare System	Provider	$552.25K
Sep 17	Ambry Genetics	Provider	$700K
Oct 29	**Lehigh Valley Health Network**	**Provider**	**$800K**

$800K

plus a three-year corrective action plan. OCR's 22nd ransomware enforcement action.

- **2023 BlackCat attack,** 248,359 individuals; Lehigh Valley declined to pay and the data was leaked.
- **OCR cited:** no accurate, thorough risk analysis; no regular review of information system activity; untimely breach notice to individuals and HHS.
- **Context:** a separate $65M class action settled in 2024.

2026 total: 10 actions, $3.78M. All 10 cite risk analysis; two of the last three also cite late notification.

Sources: HHS OCR press releases; Becker's Hospital Review; HIPAA Journal; Up from 9 actions and $2.98M in October's briefing.

HTI-5 Final Rule: Certification Shrinks, So Vendor Commitments Matter More

What the final rule did

- **Keeps** the privacy and security criteria in § 170.315(d), a baseline for now. ONC says future rulemaking may remove or update them.
- **Removes** the criteria for sending and receiving summary-of-care records tagged as restricted. Few products were certified, and vendors are not required to remove the functionality.
- **Removes** source-attribute and risk management requirements for predictive AI decision support.

A vendor's roadmap now matters more than its certification, especially for AI.

What to expect from EHR vendors

Sensitive data and privacy

1. Keep sensitive-data labeling and segmentation, and commit to it in the contract, certified or not.
2. Preserve, display, and apply restricted labels on incoming records, including downstream.
3. Make consent and disclosure restrictions travel with exported records or be clear where protection ends.
4. Give advance written notice and time to assess before changing or retiring privacy features.

AI transparency and oversight

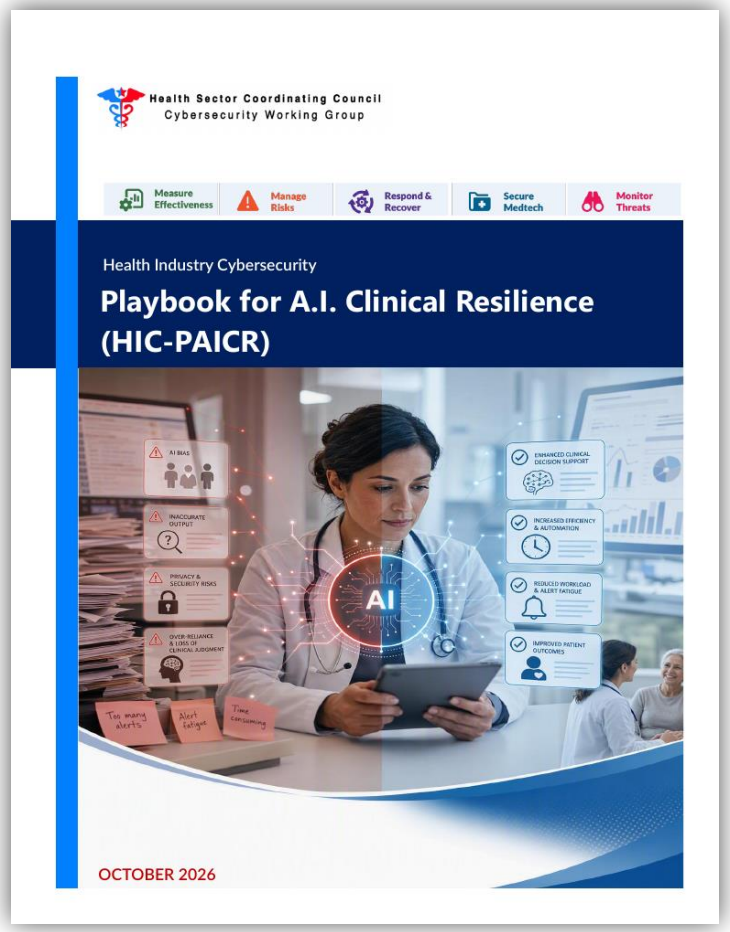
5. Be transparent about intended use, training data, validation, limitations, and bias testing.
6. Monitor AI after deployment, share findings, and report model updates or performance changes.
7. Give clinicians visibility into when AI informed a recommendation and let organizations govern its use.

8. Make vendors prove it in your environment, on real exchange workflows, with privacy, compliance, clinical, and IT leaders together.

Sources: ONC HTI-5 final rule (Oct 26, 2026); Clearwater analysis. Not legal advice.

AI Clinical Resilience

HSCC Playbook for A.I. Clinical Resilience / October 2026



What it is

A healthcare sector guide for building response playbooks that protect patients when AI fails or comes under attack.

Applies across inpatient, acute care and outpatient workflows. Connects AI risk assessment with clinical safety, incident response and care continuity.

Clearwater

Source: HSCC HIC-PAICR, October 2026, pp. 3–9

Key steps for healthcare leaders

AI response planning must protect patient safety and preserve care delivery.

1	**Inventory and prioritize AI in care**	Map AI touchpoints, data flows and dependencies. Focus dedicated playbooks on patient harm potential and autonomy.
2	**Monitor clinical failures and cyber threats**	Address model drift, bias and unsafe outputs alongside attacks. Define measurable triggers for each clinical use case.
3	**Establish shared response ownership**	Align clinical leaders with security, privacy and vendors. Decision rights follow who controls the affected component.
4	**Validate fallback and return to service**	Assess clinical risk before isolation. Restore vendor-controlled AI only after technical release and local clinical validation.
5	**Exercise and improve the playbooks**	Integrate with existing incident response. Test escalation and downtime procedures, then track response and corrective actions.

Source: HSCC HIC-PAICR, October 2026, pp. 8–18

HEALTHCARE'S CYBER BRIEFING

Preparing for Disruptions in AI-Assisted Clinical Care

FEATURING:



Dave Bailey

VP of Consulting Solutions & Strategy, Clearwater



Dr. Benoit Desjardins

Professor of Radiology, University of Montreal; Chief Medical Cybersecurity Officer (CMCO) and Chief Medical Information Officer (CMIO) in Radiology, CHUM

Clearwater

Q&A

Type your questions in the Q&A box.

Clearwater

Upcoming Webinars

Healthcare's Cyber Briefing

December 3

12:00 - 1:00 PM CT

Healthcare's Cyber Briefing

Register here

- Last session of the year featuring:
  - Chris Tyberg, Abbott
  - Greg Garcia, Executive Director, Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group

Upcoming In-Person Events



Learn more



Learn more



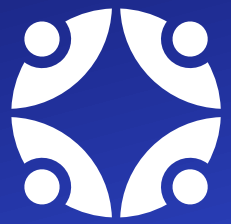
Learn more

Clearwater

We are here to help.

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

Clearwater



Clearwater

Healthcare–Secure, Compliant, Resilient

clearwatersecurity.com

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.