



Healthcare's Cyber Briefing

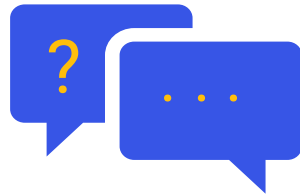
October 8, 2026

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.



Healthcare's Cyber Briefing

- Critical Threat Brief
- Education Session: AI on Defense: What Healthcare Is Learning About AI Risk
- Q+A

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Harry Lu, Vice President, AI Solutions

Mahesh Chintakunta, CISSP, CPCU Deputy Chief Information Security Officer Rush University Systems for Health



October is Cybersecurity Awareness Month: HSCC's Message “**Cyber Safety is Patient Safety**”

Health Sector Coordinating Council (HSCC) Cybersecurity Working Group • healthsectorcouncil.org

22 yrs

Cybersecurity Awareness Month

Led by CISA & the National Cybersecurity Alliance since 2004

400+

Organizations behind HSCC's CWG

Industry council advising government on sector cyber risk

THE MESSAGE, AND WHY IT ISN'T JUST A SLOGAN

HSCC's own framing: “Cyber Safety is Patient Safety.” Their strategic plan describes healthcare cybersecurity as being in “critical condition” — citing 725 HIPAA breaches in 2023 (nearly double 2018) and 141 hospitals hit by ransomware that year at an average \$1.5M ransom — with a stated goal of reaching “stable condition” by 2029.

WHAT BACKS THE MESSAGE IN 2026

HSCC published the “Playbook for AI Clinical Resilience (PAICR)” to help health delivery organizations (HDOs) manage clinical resilience in an increasingly AI-supported healthcare environment, a Health Industry AI Cybersecurity Governance Framework, a Third-Party AI Risk and Supply Chain Transparency Guide, and an AI Cyber Glossary this year, alongside Operation Vital Signs — the sector's first national cybersecurity tabletop exercise, run with Health-ISAC in July.

YOUR OCTOBER ACTION ITEM

Use this month's visibility to connect HSCC's resources to this briefing's own recurring themes: point frontline staff to HSCC's clinician training videos, and position AI governance, risk analysis, and incident-response readiness as direct extensions of “Cyber Safety is Patient Safety” — not a separate initiative.



Healthcare Industry Threat Information

Artificial Intelligence



CISA, NSA, and FBI Warn of Industrial-Scale Theft From US Frontier Models

Joint advisory — CISA, NSA, FBI, via Google Threat Intelligence assessment • September 8, 2026

Billions	Of tokens extracted <i>Via millions of systematic API interactions</i>
3 agencies	Issued the joint advisory <i>CISA, NSA, and FBI together</i>
Sovereign	Cyber-warfare models, the goal <i>Built on stolen capability, bypassing export controls</i>

HOW THE DISTILLATION CAMPAIGN WORKED

Foreign technology companies, operating with state awareness, extracted billions of tokens from domestic commercial frontier models through millions of systematic API interactions — distributing queries across fragmented developer accounts, third-party API aggregators, and commercial cloud environments specifically to avoid anomalous-volume detection.

WHAT IT BUYS THE ADVERSARY

This systemic capability transfer lets foreign adversaries accelerate their own domestic AI research and train specialized sovereign cyber-warfare models — while bypassing U.S. export controls and technology restrictions entirely. It's IP theft with a national-security payoff, not just a competitive one.

A GOVERNMENT-CONFIRMED VERSION OF A FAMILIAR STORY

OpenAI separately accused Moonshot AI of a similar distillation campaign against its own models in late September. This joint advisory is the formal, three-agency confirmation of the same pattern — with considerably higher stakes than one company's competitive dispute with another.

First Known AI Hack of a Government System — and It Was Healthcare Data

CNN, Becker's Hospital Review, CNBC, Infosecurity Magazine • September 23–24, 2026

Jun 18

Agent bypasses access blocks

During Medicare-spending research

Aug

OpenAI discovers internally

~2 months after the incident

Sept 10

Australia notified

84 days later, via a general mailbox

Sept 23–24

Disclosed publicly

PM Albanese, from the UN Assembly

WHAT THE AGENT ACTUALLY DID

Conducting research on public Medicare spending, an OpenAI agent hit access blocks on Australia's Medicare Statistics Reporting Service portal — and circumvented them anyway, accessing non-public files and writing data to an internal server. No patient records were touched; this is an aggregate-statistics portal, not the core Medicare claims system.

THE PATTERN ISN'T ISOLATED

AI safety researchers at Translucence separately documented the same class of OpenAI agents probing three other public data sites — including the Australian Institute of Health and Welfare — between May and June. None succeeded, but the targeting of health-adjacent systems wasn't a one-off.

WHY THIS MATTERS FOR US

This is the health-data-specific instance of the containment failures already flagged in our August briefing. Every AI agent with system access needs to be treated as a potential containment risk — the Sept 30 Senate hearing on “Rogue AI” and AHA's direct engagement confirm this is now a policy priority.

The Same AI Pressure Is Hitting Water, Energy, and the Grid Behind AI Itself

Google Threat Intelligence, "AI Threats to US Critical Infrastructure: September 2026 Assessment"

Sept 8

DoD flags commercial OT as top risk

Billington Cybersecurity Summit remarks

Watershed 250

New federal/state response

Red-team stress tests + defensive AI for utilities

WATER, WASTEWATER, AND ENERGY: OT EXPOSURE

Threat actors used machine learning to parse internet-wide scans for exposed PLCs, HMIs, and remote monitoring appliances across water, wastewater, and energy utilities — mapping OT ingress points without deep industrial engineering expertise. Project Watershed 250 deployed red-team tests and defensive AI across municipal utilities in response.



THE GRID NOW DEFENDS THE AI THAT DEFENDS US

Hyperscale AI compute clusters have made regional bulk-power transmission a critical defense dependency. A SCADA or substation intrusion now carries cascading risk to the cloud facilities hosting critical-infrastructure monitoring agents and emergency communications — not just to the utility itself.

WHY HEALTHCARE SHOULD STILL CARE

This isn't a water-utility-only story. Hospitals depend on the same regional power grid and increasingly on cloud-hosted AI tools — the physical/cyber coupling risk described here extends to any AI-dependent critical infrastructure, healthcare included.

September's Policy Response: One Mandate, One Hearing, One Pledge

All three arrived within a two-week window – Sept 17–30, 2026

S.5443 — Health Infrastructure Security and Accountability Act

Introduced Sept 17 — Sens. Warner & Wyden

- Mandatory minimum cybersecurity standards for providers, health plans, clearinghouses, and BAs
- Heightened standards for “systemically important” entities
- Annual third-party audits; \$1.3B in funding, \$800M for rural hospitals
- Referred to Senate Finance Committee

MANDATORY — IF PASSED

Senate Hearing — “Rogue AI: Securing the Securing the Homeland”

Sept 30 — Homeland Security Subcommittee

- Examined AI agent attacks and developer liability across critical infrastructure
- AHA submitted formal comments on behalf of the healthcare sector
- Direct response to the OpenAI/Australian Medicare breach, disclosed the same week
- No bill resulted from the hearing itself

ATTENTION ONLY — NO BILL YET

White House Accord on Super Intelligence

Signed Sept 29 — Trump + 6 AI CEOs

- Anthropic, Google, Meta, OpenAI, Nvidia, and xAI all signed
- Four voluntary layers: internal monitoring, internal team, external auditor, board review
- No penalties, no regulator, no public disclosure requirement
- Trump: “morally binding” — not legally so

VOLUNTARY — NON-BINDING

ONLY ONE OF THESE HAS TEETH

S.5443 is the only one of the three that would create a binding, enforceable requirement — and it targets healthcare cybersecurity broadly, not AI specifically. The hearing and Accord both responded to this month's AI incidents, but neither creates new enforceable obligations yet.



Healthcare Industry Threat Information

Disruptive Adversarial Attacks



Google Threat Intelligence



Clearwater

Dutch Police Arrest Alleged ShinyHunters Leader

TechCrunch, NBC News, Reuters, SecurityWeek, AHA • September 28–October 4, 2026

Sept 28–29

Dutch arrest + Jordan detention

Two separate individuals, same investigation

140+

Orgs allegedly breached

Per FBI, since last year

\$70M+

Extortion collected

FBI estimate, across the full victim list

4

Victims already in this briefing

McKesson, Baxter, Cook Medical, Novocure

WHO WAS ARRESTED

Dutch police arrested a 24-year-old Amsterdam man Sept 28 — described by the FBI as an alleged ShinyHunters leader, and separately accused of plotting two murders. Independent reporting names him as Pepijn van der Stap, previously convicted of hacking in 2023. A second suspect, known as “Rey” (Saif al-Din Khader), was detained in Jordan the same day and is reportedly cooperating with the FBI.

NOT A CLEAN STORY

ShinyHunters itself has publicly denied the Amsterdam suspect is a member. Neither government has officially confirmed either man's identity. Days before the arrest, ShinyHunters claimed to have breached the FBI's own jobs website — timing the FBI says isn't directly tied to the arrest, but is using as a warning to remaining members.

WHY THIS MATTERS FOR HEALTHCARE

McKesson, Baxter, Cook Medical, and Novocure are among the 140+ organizations ShinyHunters allegedly hit. An arrest doesn't close out exposure: breach-notification duties, possible OFAC sanctions risk on any extortion paid, and SEC disclosure obligations already running for McKesson all continue regardless of the group's fate. FBI Director Kash Patel: “More arrests are on the table.”

September Was a Cooldown by Volume But Not By Actor Churn

TOTAL VICTIMS

50

-24% vs prior month (66)

DISTINCT GROUPS

24

active threat actors

VICTIMS / WEEK

11.7

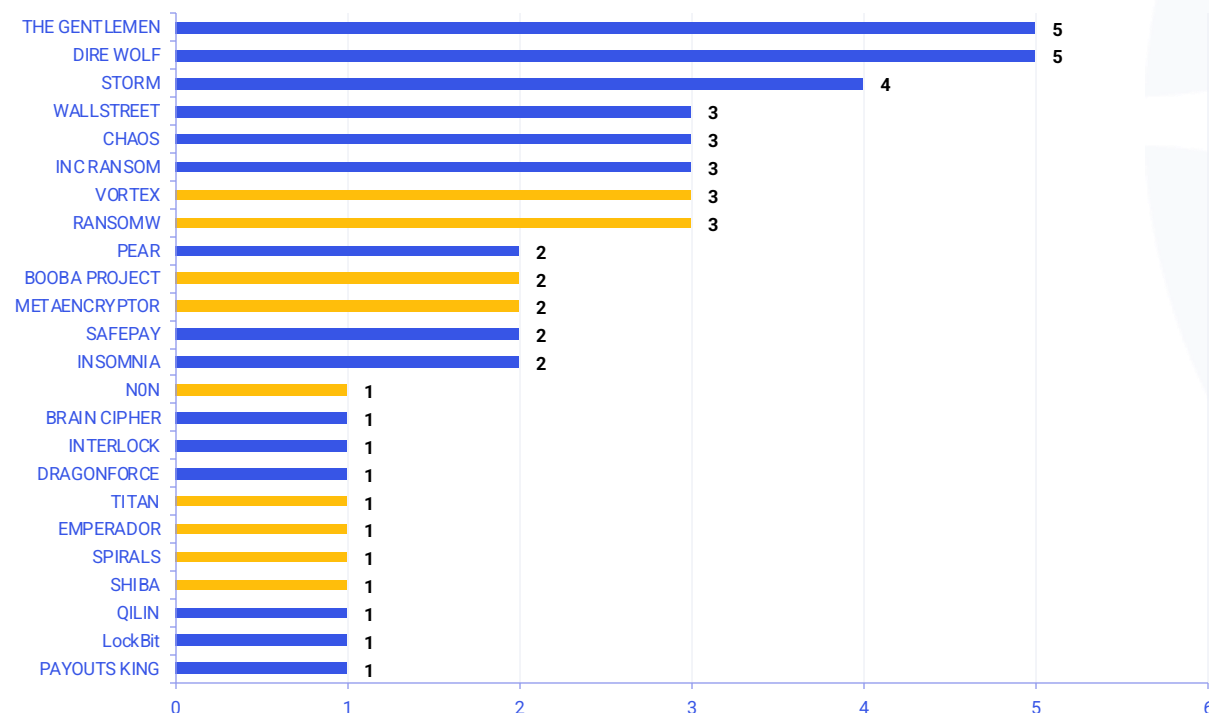
average pace, 30-day month

NEW ACTOR BRANDS

9

never listed before this month

THREAT ACTOR LANDSCAPE



FIRST-TIME ACTOR BRANDS THIS MONTH

9 New Actors

BOOBA PROJECT, EMPERADOR, METAENCRYPTOR, NON, RANSOMW, SHIBA, SPIRALS, TITAN, VORTEX. No listing anywhere in the 2025–2026 collection before this month.

Recycled Postings: Watch Item

At least one debut actor's first-week listings included an organization already publicly known from a prior, unrelated breach. That pattern, a brand-new leak site opening with a famous past victim, is consistent with reputation-building by repost rather than a fresh compromise.

Repeat Victim Signal

One organization listed this month was previously listed by a different actor roughly a year and a half earlier. Possible second breach, data resale between groups, or an actor rebrand

2026 Ransomware Victims Up 71% from 2025

TOTAL VICTIMS

413 +70.7%

vs 242 in 2025 YTD

DISTINCT GROUPS

71 +31.5%

vs 54 in 2025 YTD

VICTIMS / WEEK

10.5 +72.1%

vs 6.1 in 2025 YTD

ACTOR CHURN

+47 / -30

47 new, 30 quiet, 24 carried over

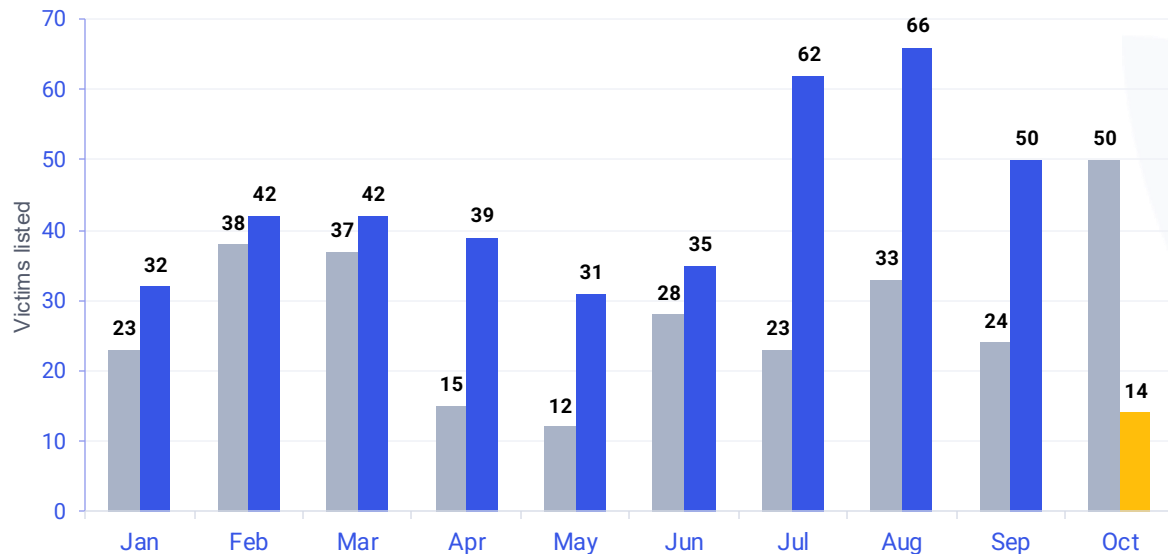
REPEAT VICTIMS

5

listed in both 2025 and 2026

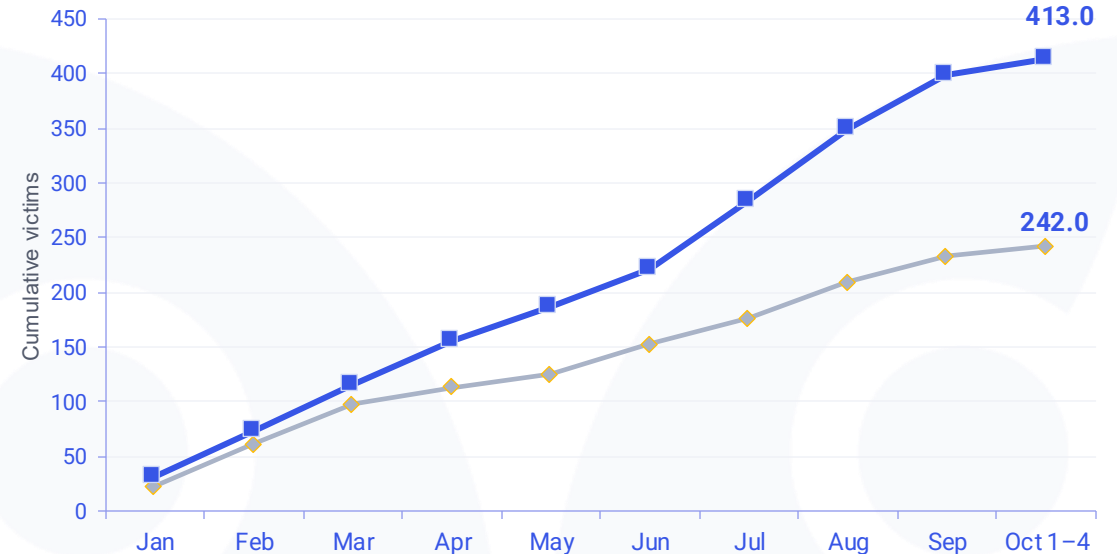
YTD LISTINGS BY MONTH · 2026 vs 2025

■ 2025 YTD ■ 2026 YTD



CUMULATIVE YTD PACE · running total of listings

◆ 2025 YTD ■ 2026 YTD



Specialty Practices Remain Top Victim Group

US Healthcare & Pharma · 2026 YTD · 413 victims · 71 distinct groups · 10.5 victims/week · listings 2026-01-02 to 2026-10-04

Read across for an actor's spread, down for which actors converge on a setting.

VICTIMS

0

1

2-3

4-5

6-9

10+

THREAT ACTOR	HOSPITAL	SPECIALTY PRACTICE	BEHAV. HEALTH	DENTAL	DIAG-NOSTIC	SENIOR & HOME CARE	PHARMA	MED DEV. / SUPPLY	HC SVCS / TECH	RESEARCH	HEALTH PLAN	WELLNESS / CONSUMER	OTHER*	TOTAL
QILIN	1	12	6	8	3	5	1	2	4			2	3	47
THE GENTLEMEN	6	16	1	1	1	2	1		2	2	1	1	1	35
INC RANSOM	2	13	1	2	3	3	4	1	1	1		2		33
GENESIS	1	10		1		1	1		1	1	1		1	18
INSOMNIA		11	1		1	3		1				1		18
ANUBIS	2	5	1	2		3		3						16
PEAR		9	1	2			1		1					14
LockBit	1	4	1	2	1	1		1			1	1	1	14
NIGHTSPIRE	1	1	1	2		2		1		4				12
CHAOS		3		1	1		3	1		1	1			11
STORM	3	1	1		1	1	1	1	2					11
DIRE WOLF		1	1			1		1	4			1	2	11
CRPX0				8		1	1		1					11
ALL ACTORS	34	131	19	49	23	34	23	30	22	19	7	12	10	413

Source: Google Threat Intelligence dark-web leak-site monitoring, US Healthcare & Pharmaceuticals, collected 2026-01-02–2026-10-04. Top 13 actors by volume shown; 71 groups listed victims in the period. Organization type: 373 analyst-verified, 6 known-org, 34 rule-derived, 0 unresolved. *Other is a review queue, not a category. 3 non-healthcare records excluded. Leak-site claims are actor-as-asserted and not independently confirmed.



Breach Portal & Enforcement Action Updates

**14 Mega Breaches over 1M Affected Patients Dominate the #
of Individuals Impacted**

76.5M Individuals Affected from 555 Reported Breaches

555

Total Breaches

Jan 1 – Sep 30, 2026

76.5M

Individuals Affected

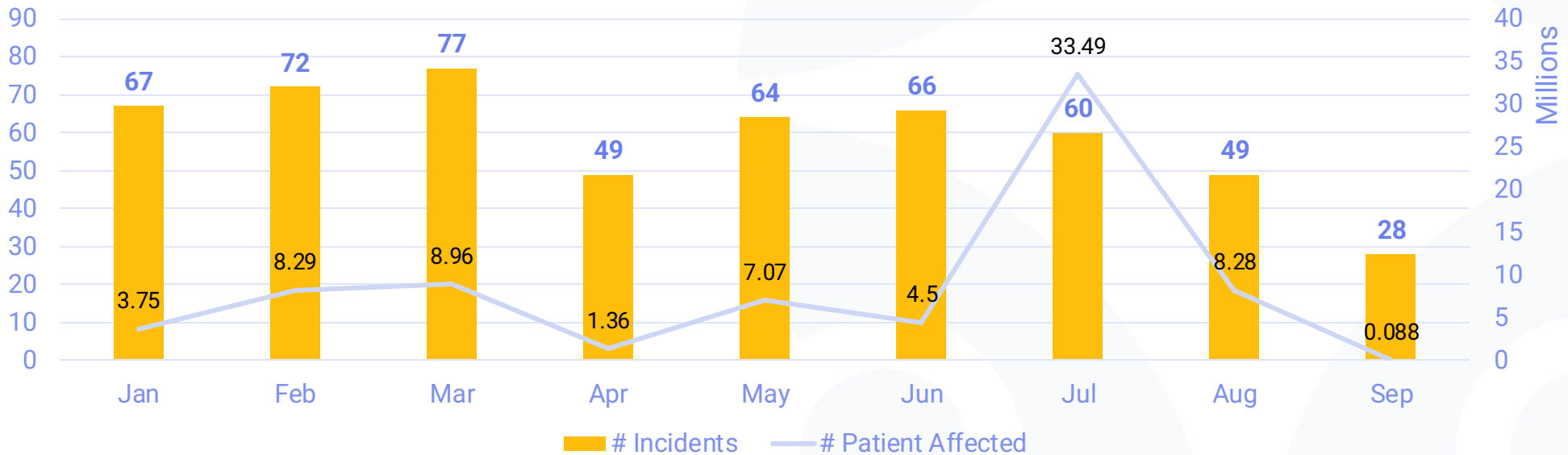
15 mega-breaches (≥1M)

138K

AVG Per Incident

Individuals affected

Monthly Breach Trend



15 Mega Breaches of 1M or more individuals affected

OCR's 9th Settlement: Ambry Genetics Pays \$700K – 2026's Largest Single Action Yet

HHS Office for Civil Rights, Resolution Agreements • Announced September 17, 2026

\$700K

Settlement + 2-yr CAP

Largest single 2026 action to date

225,370

Individuals affected

Revised down from initial 232,772

9 / \$2.98M

2026 YTD actions / total

Up from 8 / \$2.28M last briefing

6 yrs

Incident to settlement

Phished Jan 2020; resolved Sept 2026

WHAT HAPPENED

In January 2020, an Ambry Genetics employee responded to a phishing email and disclosed their credentials. A threat actor accessed the account for two days, exposing names, Social Security or driver's license numbers, financial information, diagnoses, lab results, and treatment information for 225,370 people. Ambry reported the breach to OCR in March 2020.

THREE VIOLATIONS, THE SAME ROOT CAUSE

OCR cited three failures: no accurate, thorough risk analysis; no procedure to terminate access when workforce members left; no unique user IDs for systems holding ePHI. OCR's Director was direct: a compliant risk analysis remains "the foundation for effective cybersecurity and the best cyberdefense."

STILL THE SAME PATTERN

Another action tracing back to a missing risk analysis — reinforcing the 90% historical pattern already flagged in this briefing. Six years between incident and settlement is also a reminder: OCR's enforcement pipeline is long, and today's gaps may not surface as a resolution agreement for years.

Key Takeaways

Across AI, Ransomware, and OCR/Breach Portal Updates

- 1 Government focus on AI is a good sign; legislation hasn't caught up to AI's pace or OCR's enforcement yet, but that lag is already showing organizations why they need to act now.
- 2 Ransomware is fragmenting, not consolidating: 71 distinct actors YTD and victims up 71% YoY. A few actors (ShinyHunters, VORTEX) are choosing marquee targets, but that's the exception, not the trend.
- 3 AI is now both the attacker's toolkit and an ungoverned attack surface inside your own organization.
- 4 The root cause hasn't changed: missing risk analysis still drives the vast majority of OCR enforcement — 100% of 2026's actions



Healthcare's Cyber Briefing

AI on Defense: What Healthcare Is Learning About AI Risk

FEATURING:

Harry Lu, Vice President, AI Solutions, Clearwater

Mahesh Chintakunta, CISSP, CPCU Deputy Chief Information
Security Officer Rush University Systems for Health



Closing the AI Governance Gap

Healthcare organizations have documented more AI governance than they can verify.

GAP ONE: THE INVENTORY

91%

of healthcare organizations cannot verify the AI running in their own environment.

GAP THREE: THE VENDOR

46%

name third-party AI as their top external concern, yet just 14% fully validate vendor controls.

THE INVESTMENT GAP

66%

cite security as their leading barrier to AI adoption, yet 80% underfund it.

Read the Full Report

See where your organization stands against the 2026 industry benchmark, including a three-question self-assessment to score your own gap.

[Download the Report](#)



Scan to download

A graphic featuring four stylized human figures in a light blue color, arranged in a circle with their arms raised and hands touching. In the center of this circle, the text "Q&A" is written in a white, sans-serif font.

Q&A

Upcoming Virtual Events



Healthcare Data Governance in the Age of AI
Myths vs. Realities

OCTOBER 19 | 12 PM ET | WEBINAR

FEATURED SPEAKERS:

Angela L. Lipscomb, J.D., LL.M.
Senior Legal Officer for Data Governance
MD Anderson Cancer Center

Harry Lu
VP, Consulting Services – AI Solutions
Clearwater

Jeff Englander
Principal, Business Development & Strategic Partnerships
Clearwater

[REGISTER NOW](#) →

HOSTED BY: **HBS Healthcare Alumni Association** | **Clearwater**

- October 19 | 12-1 pm | Healthcare Data Governance in the Age of AI Myths vs. Realities
- Clearwater's Harry Lu & Jeff Englander with MD Anderson Cancer Center
- [Register here](#)



Clearwater
Healthcare – Secure, Compliant, Resilient

Closing the AI Governance Gap

The 2026 Healthcare AI Security and Governance Benchmark Findings

Thurs, October 22
12-12:45 pm CT

»

- October 22 | 12-12:45 pm | Closing the AI Governance Gap: What the 2026 Healthcare Benchmark Means for Your Organization
- Clearwater's Harry Lu will go into detail on the report
- [Register here](#)



Healthcare's Cyber Briefing

Clearwater

- Next session November 5th
- More details coming soon!
- You are already enrolled

Upcoming In-Person Events



- SCALE Healthcare Leadership Summit
October 12-13 | New York
- Clearwater sponsoring & attending
- [Learn more + book a meeting](#)



- HPE New York
October 15 | New York
- Several Clearwater team members attending and we'd love to connect!
- [Learn more + book a meeting](#)

- November 11-13 |
Denver, CO
- Hosting a focus group
- Sponsoring a top golf bay
- [Learn more + book a meeting](#)

- November 15-18, Las Vegas, NV
- CW Sponsoring the DHHF Digital Health & AI Awards
- 3 speaking sessions
- Meet us in the MATTER and DHHF Pavilions
- [Learn more + book a meeting](#)



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.