Healthcare's Cyber Briefing

July 9, 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.

Clearwater

Healthcare's Cyber Briefing

- Critical Threat Brief
- Education Session: Recovery Under Pressure: What Separates Weeks from Months in Healthcare Incident Response
- Q+A

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Heather Hanson, Manager, Resiliency Services

Healthcare Industry Threat Information

Relevant Threat Information for Healthcare

Google Threat Intelligence

Clearwater

Artificial Intelligence

AI is Moving in 3 Directions at Once

A New Attack Surface

The chatbots, copilots, and AI agents' healthcare organizations already deploy for productivity are being manipulated, chained, or tricked into acting against the very systems they're meant to protect.

A Force Multiplier for Nation-States

Nation-state actors are using AI to scale target identification, credential theft, and social engineering — increasing the speed, reach, and precision of state-sponsored operations against the sector.

A Capability Outpacing Defenses

Frontier AI vulnerability-discovery capability is advancing faster than most healthcare organizations can adapt their defenses, compressing the time between disclosure and exploitation.

Individually, each of these developments is serious. Together, they compound into a threat trajectory healthcare leadership cannot address with yesterday's playbook — reinforcing the case for building AI governance, vulnerability management, and incident response capacity now.

Artificial Intelligence

Frontier AI Model Day: The Clock Healthcare Is Racing

Frontier AI Model Day — the day frontier, Mythos-class AI vulnerability-discovery capability reaches the adversary groups that target the U.S. Healthcare and Public Health sector — and they begin using it.

1

Mythos NSA Red-Team Exercise

Anthropic's frontier model reportedly found vulnerabilities across classified systems in hours, not weeks.

2

Alibaba-Linked Distillation of Claude

28.8M exchanges used to extract vulnerability-hunting capability from a frontier model.

3

AI-Compressed Attacker Tradecraft

Average breach-to-lateral-movement breakout time is down to just 48 minutes.

!

FRONTIER AI MODEL DAY

The day this capability reaches the adversary groups targeting healthcare — at scale.

"The timeline is not years, it is months."

— Five Eyes intelligence alliance (US, UK, Canada, Australia, New Zealand), joint statement on frontier AI cyber capabilities, June 22, 2026. Signed by NSA's Director of the Cybersecurity Directorate and the acting CISA Director.

U.S. Policy Response: Review, Restriction, and Reversal

A Formal Review Process

- Jun 2, 2026 — White House executive order “Promoting Advanced AI Innovation and Security” creates a voluntary “covered frontier model” review process.
- Directs CISA to expand access to AI-enabled defense tools for critical infrastructure, including rural hospitals.
- Orders DOJ to prioritize AI-enabled cybercrime enforcement.

An Export Ban, Then a Reversal

- Jun 12, 2026 — Claude Fable 5 and Mythos 5 suspended worldwide under a Commerce Department export-control order — the first real-world government-mandated shutdown of a deployed frontier model.
- The trigger: a reported jailbreak surfaced exploit-adjacent output from the models.
- Jun 30 – Jul 1, 2026 — Commerce lifted the export controls; Anthropic restored access to both models.

The lesson for healthcare isn't the specific model or the specific order — it's that frontier AI is now squarely a matter of national security policy, with direct implications for AI vendor dependency, contract risk, and continuity planning.

What is Means for Healthcare Leadership

1 Govern AI Like Any Critical Vendor Dependency

Inventory AI tools embedded in clinical, administrative, and vendor workflows. Review AI vendor contracts for suspension, failover, and data-retention provisions — generic “force majeure” language is not sufficient.

2 Compress Vulnerability Management & IR Timelines

Benchmark your patch and response cycle time against AI-assisted attacker speed, not historical adversary timelines. Treat a 48-minute breakout time as the new baseline threat model, not the exception.

3 Elevate Frontier AI Proliferation to a Board-Level Risk

Frontier AI Model Day is a matter of when, not if. Build AI governance, vulnerability management, and incident response capacity now, while the window still favors the defender.

Breach Portal Updates

2026 YTD HIPAA Breach Report

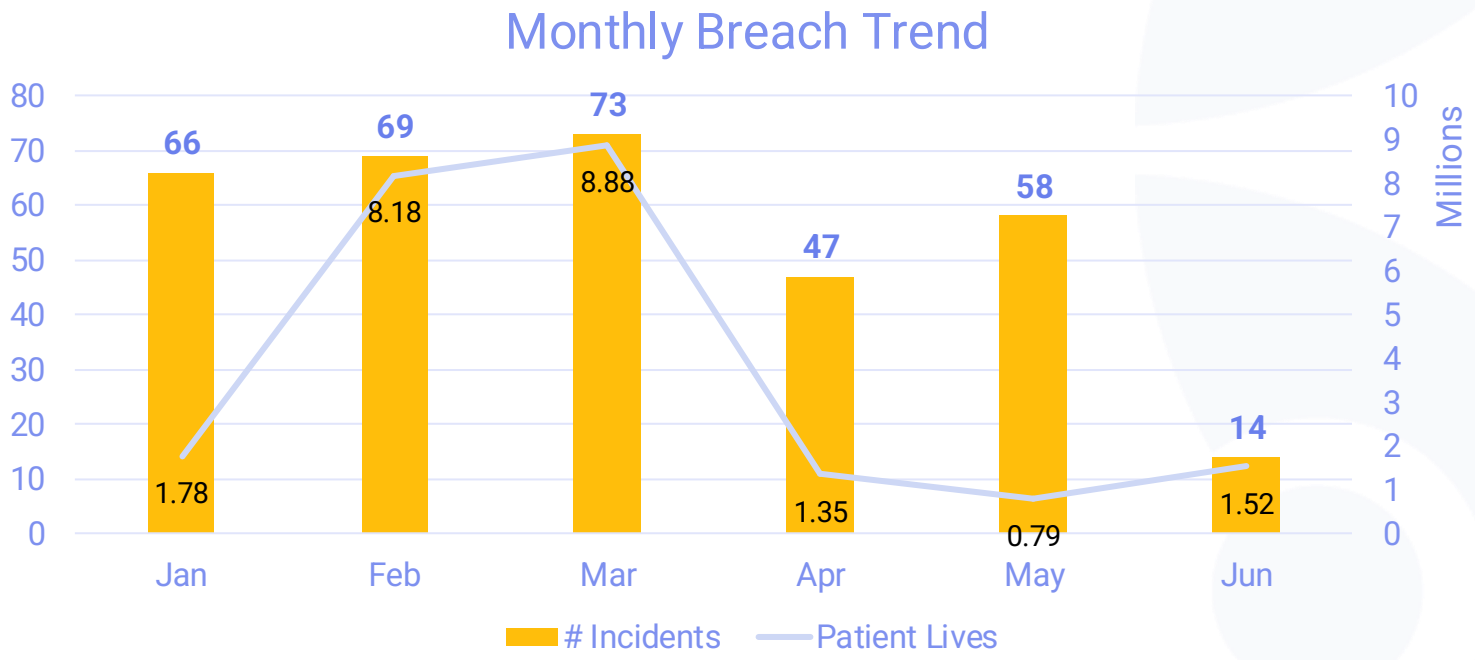
Clearwater

A Handful of Mega-Breaches Drive Most of the Exposure

327
Total Breaches
Jan 1 – May 15, 2026

22.5M
Individuals Affected
5 mega-breaches (≥1M)

94%
Hacking/IT Incidents
280 of 327 breaches



- **A handful of mega-breaches drive most of the exposure**: the top 5 incidents alone (TriZetto Provider Solutions, QualDerm Partners, Nacogdoches Memorial Hospital, Navia Benefit Solutions, and NYC Health + Hospitals) **account for over 13M of the 22.5M individuals affected YTD**.
- **In June, one breach drove almost all the impact**: Xsolis, Inc. (a Business Associate, TN) alone accounts for **1.4M of the 1.52M individuals affected — 92% of the month's total.**

Clearwater

Source: HHS OCR Breach Portal | Active + Archive exports through May 15, 2026

Ransomware Updates

June Resurgence, Top Actors, and Targeting Patterns

Clearwater

Ransomware Data Leaks

223 Reported Victims Through Q2 with a June Resurgence

Healthcare ransomware activity showed no sign of easing in the first half of 2026, with 223 victims tracked across 44 distinct threat actor groups

223

Healthcare & pharma victims posted, Jan–May 2026

44

Distinct threat actors observed targeting the sector YTD

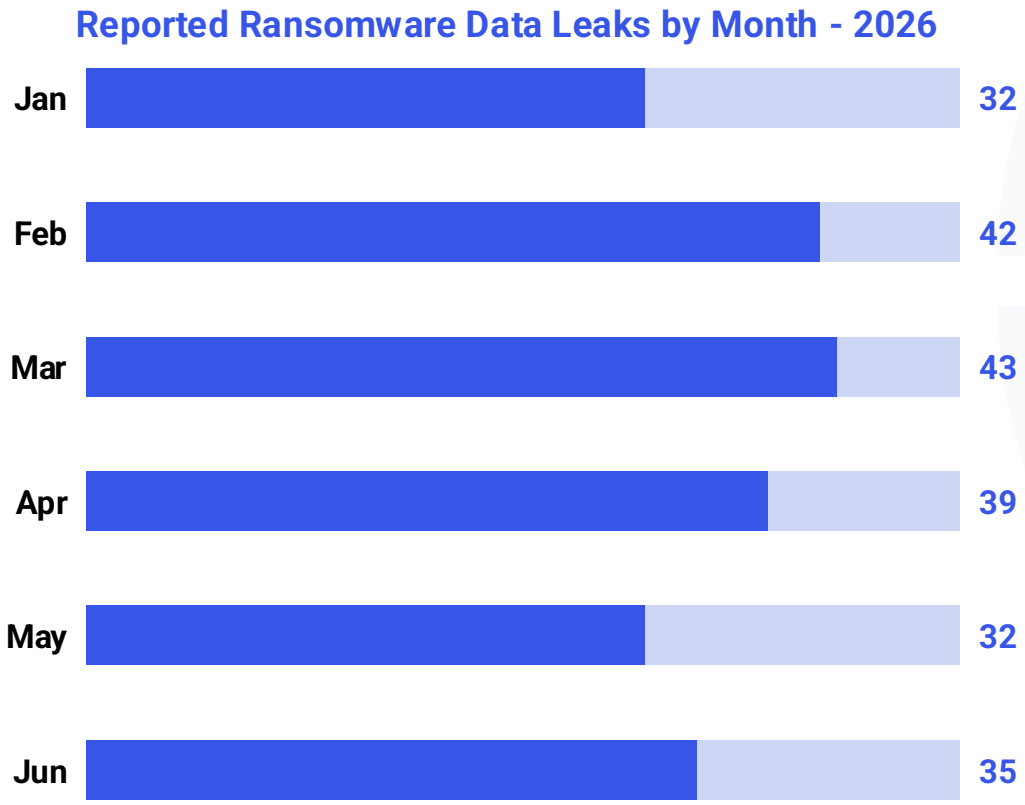
35

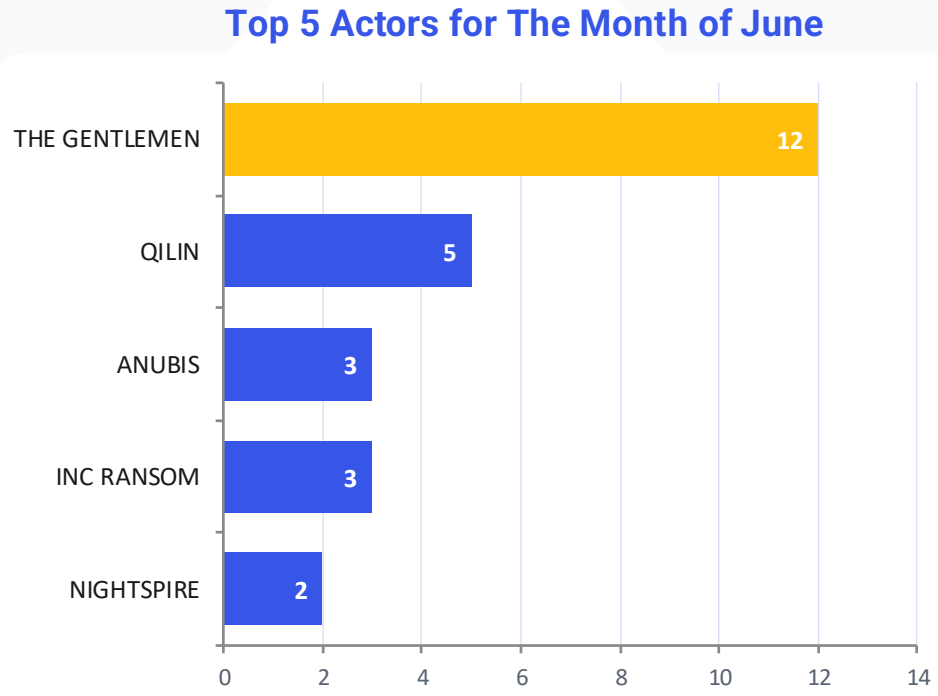
Victims claimed in June up from 32 in May

The 6-month picture: steady volume, persistent targeting of small specialty practices, and a churning roster of attackers behind a small group of consistent leaders.

June Rebounds Led by The Gentlemen with 12 Victims

Activity peaked in February and March before declining briefly through April and May, only to rebound sharply in June, driven primarily by THE GENTLEMEN surging to 12 victims in a single month





Ransomware Data Leaks

Specialty Practices Remain the Most Consistently Targeted Segment of the Healthcare Sector, Representing 61% of All Victims

Threat Actor	Specialty Practice	Hospital	Dental	Diagnostic	Pharma	Research	Senior Care
QILIN	25	1	6	2			1
THE GENTLEMEN	12	3	1	1	1	1	
INC RANSOM	10	1	1	3	3	1	
INSOMNIA	10			1		1	1
NIGHTSPIRE	4	2	2			3	
LockBit	7	1	2	1			
GENESIS	7	2	1		1		
SINOBI	4		2	1		2	1
ANUBIS	6	1	2				
AKIRA	4		2	1	1		
CMD ORGANIZATION	7						
COINBASE CARTEL	1			1		5	
WORLD LEAKS	1	3	1		1		

Clearwater

INTENSITY ▶ 1 — Low 2–3 Moderate 4–5 Elevated 6–9 High 10+ Critical

Ransomware Data Leaks

Qilin Maintains Sustained Activity Across All 6 Months

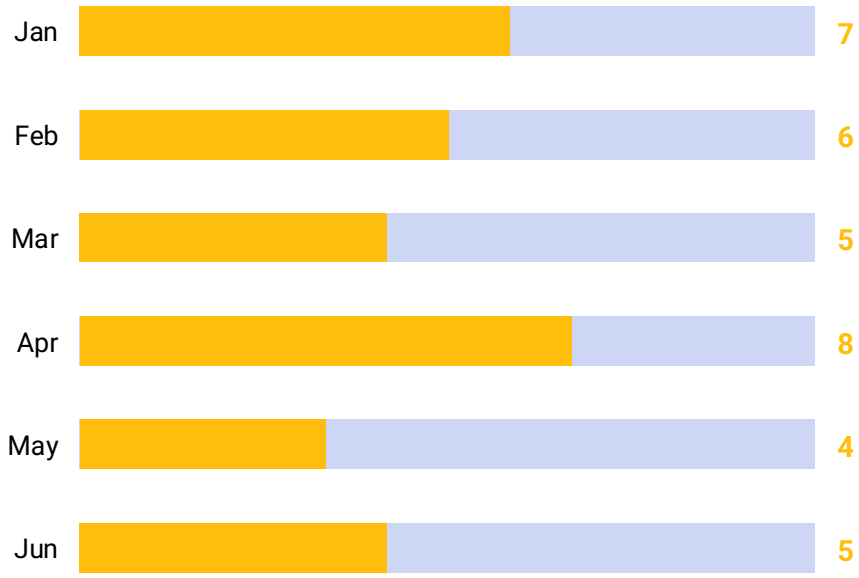
35
Victims Jan–Jun 2026

15.7%
Share of Total Listings

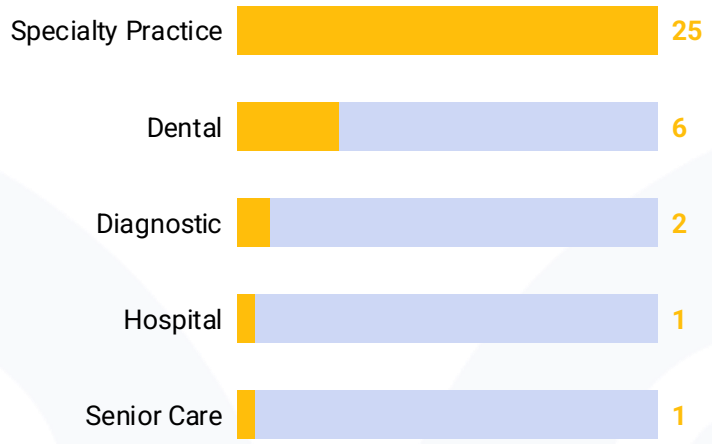
6
Active Months
of 6 monitored

Specialty
Primary Target
Specialty Practice

MONTHLY VICTIM ACTIVITY



TARGETING BY ORGANIZATION TYPE



INTELLIGENCE NOTE

QILIN maintained activity across all 6 months with no dormant periods — the only top-5 actor to do so. Their April peak (8 victims) aligns with broader Q2 escalation trends. With 35 victims across 6 months, QILIN represents the single greatest sustained threat to the healthcare sector in this dataset.

The Gentlemen Surges in June with 12 Victims

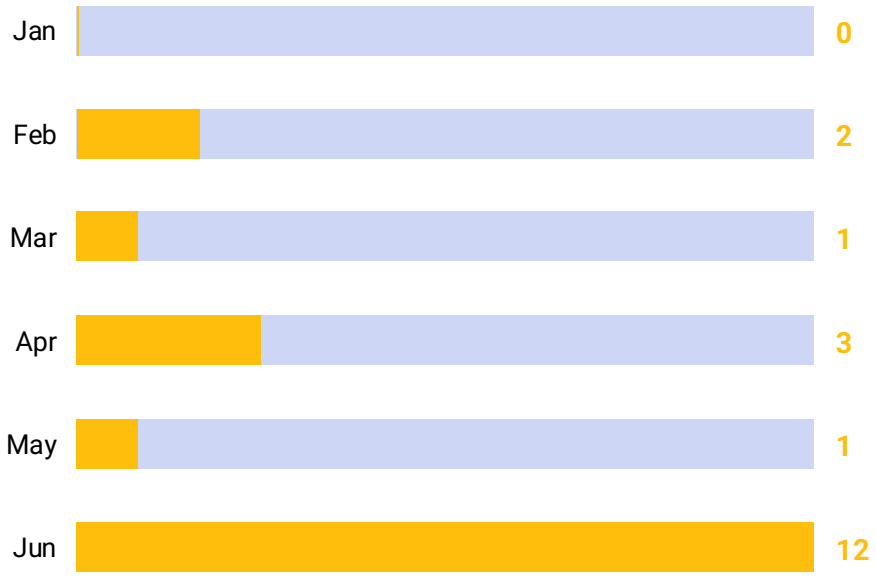
19
Victims Jan–Jun 2026

8.5%
Share of Total Listings

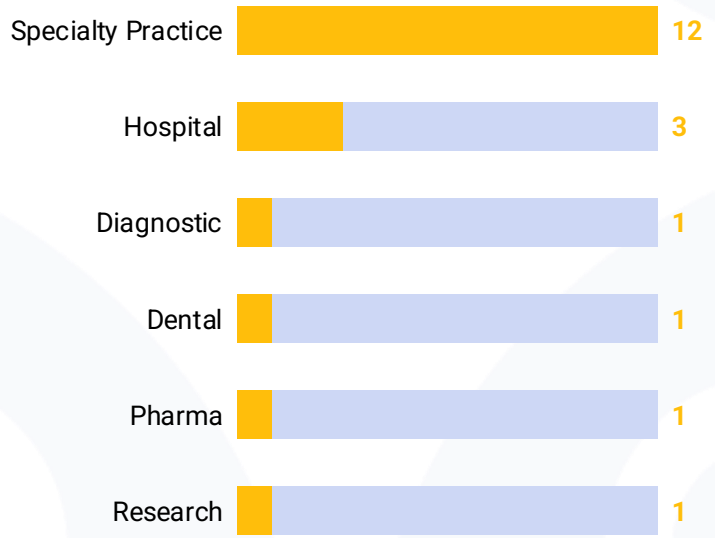
5
Active Months
of 6 monitored

Specialty
Primary Target
Specialty Practice

MONTHLY VICTIM ACTIVITY



TARGETING BY ORGANIZATION TYPE



INTELLIGENCE NOTE

THE GENTLEMEN's June surge — 12 victims in a single month — is the most dramatic single-month escalation by any actor. 63% of their total victims appeared in June alone. Their hospital targeting (3 of 19 victims, 16%) is notably elevated relative to peers and warrants close monitoring in Q3.

STOP Ransomware

Top Priorities for Identity, Access, & Infrastructure Hardening

1 Enforce Phishing-Resistant MFA

Require hardware key or FIDO2 authentication on all remote access and EHR platforms. Access broker targeting patterns confirm credentials — not unpatched systems — are the primary initial access surface for specialty practices.

Addresses: INSOMNIA, CMD ORGANIZATION

2 Audit & Rotate Privileged Credentials

Bulk-publish patterns indicate exfiltration precedes public listing by weeks or months. Treat full credential rotation and service account audits as a standing quarterly hygiene requirement, not a post-incident response.

Addresses: SINOBI, INSOMNIA

3 Segment Clinical from Administrative Networks

Isolate clinical applications, imaging systems, and EHR platforms from workstations and vendor-connected systems. Flat networks allow a single compromised endpoint to become a full clinical breach.

Addresses: THE GENTLEMEN, INC RANSOM

4 Patch Internet-Facing Systems Within 72 Hours

Apply critical CVE patches to VPNs, remote desktop gateways, and web applications within 72 hours of publication. LockBit's continued activity post-takedown confirms affiliate infrastructure outlasts law enforcement action.

Addresses: QILIN, LockBit

STOP Ransomware

Top Priorities for Identity, Access, & Infrastructure Hardening

5 Verify Offline & Immutable Backups

Test backup restoration quarterly across all critical clinical and operational systems. Backup infrastructure connected to production networks provides no meaningful protection against operators who conduct pre-deployment reconnaissance.

Addresses: All top actors

6 Deploy Continuous Dark Web Monitoring

Early leak site detection is the only realistic window between exfiltration and public disclosure. Monitoring enables breach containment and notification preparation before regulatory deadlines are triggered.

Addresses: SINOBI, INSOMNIA, THE GENTLEMEN

7 Review & Restrict Third-Party Vendor Access

Inventory all remote vendor connections with a focus on diagnostic and pharmaceutical service providers. INC RANSOM's sector targeting pattern is consistent with supply chain exploitation across connected healthcare clients.

Addresses: INC RANSOM, NIGHTSPIRE

8 Deploy 24/7 MDR with Threat Intelligence

QILIN's unbroken six-month activity and THE GENTLEMEN's surge from 1 to 12 victims in a single month confirm threats are continuous. Daytime-only or periodic monitoring creates detection gaps that active threat actors exploit.

Addresses: QILIN, THE GENTLEMEN

Key Takeaways

1. **AI is now Both the Target and the Tool**
2. **A Handful of Mega-Breaches Drive Most of 2026 Exposure**
3. **Ransomware Pressure on Specialty Practices Isn’t Easing**
4. **Bottom Line: Treat Identity, Access & IR Readiness as Urgent**

Google Threat Intelligence

Clearwater

Healthcare's Cyber Briefing

Recovery Under Pressure: What Separates Weeks from Months in Healthcare Incident Response

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Heather Hanson, Manager, Resiliency Services

- ***How operational resilience and incident response planning protect patient care, reduce downtime, and minimize financial impact.***

Why It Matters

Preparation—not luck—determines how quickly healthcare organizations recover from a cyberattack.

The Fact Is…

Patients, clients, and stakeholders don’t care how protected you are if you can’t recover safely and quickly!

Clearwater

What Separates Weeks From Months In Healthcare Incident Response

Operational Resilience Means…

- The ability to anticipate, withstand, respond to, and recover from major operational disruptions.
- Maintaining delivery of critical patient care even when systems fail.
- Assuming disruption is inevitable and planning accordingly.

Operational Core Pillars

- Service mapping
- Defined tolerance for disruption
- Continuous testing and simulation
- Third-party risk management

What Separates Weeks From Months In Healthcare Incident Response

Business Continuity vs. Operational Resilience

Operational resilience helps reduce regulatory exposure, financial losses, reputational damage, and patient safety risks.

Traditional Business Continuity	Modern Operational Resilience
▪ Protects technology and infrastructure	▪ Protects patients and essential clinical services
▪ Assumes attacks can be prevented	▪ Assumes disruptions will occur
▪ IT-focused recovery	▪ Enterprise-wide coordination across IT, clinical, legal, and operations
▪ Component testing	▪ End-to-end crisis simulations

What Separates Weeks From Months In Healthcare Incident Response

The Difference Preparation Makes
Recovery Outcomes: Prepared vs. Unprepared Organizations

Organizations with mature incident response plans recover faster, spend less, and maintain clinical operations.

With Incident Response Planning

- ✓ Automated system isolation within hours
- ✓ Immutable offline backups remain available
- ✓ Downtime procedures preserve patient care
- ✓ 53% recover within one week
- ✓ **Median recovery cost: ~$375K**

Without Incident Response Planning

- ✗ Manual organization-wide shutdowns
- ✗ Backups deleted or encrypted
- ✗ Ambulance diversions and delayed treatment
- ✗ Recovery often exceeds 21–24 days
- ✗ **Median recovery cost: $750K+**

Recovery Under Pressure

What Separates Weeks From Months In Healthcare Incident Response

What Successful Response Looks Like: Real-World Success Stories

1

Automated Detection & Isolation

- Immediate endpoint isolation
- Threat contained before reaching EHR systems
- Zero disruption to patient care

2

72-Hour Clean Rebuild

- Segmented infrastructure
- Immutable offline backups
- Standardized rebuild playbooks
- Baseline restoration in 72 hours to one week

Clearwater

What Separates Weeks From Months In Healthcare Incident Response

When Planning Falls Short: Lessons from Recent Healthcare Cyberattacks

9

MONTHS TO RECOVER

⚠ Change Healthcare (2024)

- Weak identity protection and lack of MFA
- Entire payment network shut down
- Claims testing delayed nearly one month
- Full operational recovery required approximately **9 months**

$34.2M

FINANCIAL IMPACT

⚠ Mississippi Medical Center (2026)

- All clinics were closed, non-emergency treatments and elective procedures canceled.
- Hospitals and Critical Care Units remained operational using downtime procedures.
- Financial impact of $34.2m, and data privacy investigations
- Full System Downtime of 9 days

What Separates Weeks From Months In Healthcare Incident Response

Q&A With Dave Bailey - Mythos AI and Resilience

1. Corrupt AI and Systems Integration
2. Data Leakage through AI Assistants
3. What to Consider Beyond the Foundations

RIGHT NOW	NEAR TERM	LOOKING AHEAD
Get really good at patching and incident response	Plan out how to deal with increased patching demands and incident response: Even effective plans and processes don't scale without testing, review and adjustment	Implement AI-Powered Defenses. Only AI-speed detection matches AI-speed attacks

What Separates Weeks From Months In Healthcare Incident Response

Key Takeaways

Building a Faster, Safer Recovery

- ✓ Operational resilience is the foundation of effective incident response.
- ✓ Incident response planning dramatically reduces recovery time and cost.
- ✓ Immutable backups and automated containment minimize operational disruption.
- ✓ Regular exercises validate teams can execute recovery plans under pressure.
- ✓ Cybersecurity should be viewed as a patient safety and operational continuity strategy—not simply an IT investment.

The question is no longer whether healthcare organizations will experience disruption—but whether they are prepared to continue delivering patient care when it happens.

Q&A

Clearwater

Announcing *Operation Vital Signs* – An HPH Sector Exercise

In July 2026, the Health Sector Coordinating Council (HSCC) Cyber Working Group (CWG) and Health-ISAC are hosting "Operation Vital Signs," a two-day cyber incident response and recovery exercise for the Healthcare and Public Health (HPH) Sector

All HPH Sector members are invited and encouraged to participate!

Who is invited to participate?

- ***All HPH Sector members***
- *Within organizations we are targeting any personnel involved in leading cyber incident response, associated crisis and continuity activities, recovery planning and execution, and external/sector coordination activities*

When and where will the exercise occur?

July 21-22, 2026 *(over two half-day virtual sessions)*

The exercise sessions will be preceded and followed by offline feedback forms/surveys to capture data for our report

What are the focus areas and the output?

*Within **organizations,** the focus is on response and recovery, including impacts to critical functions and patient safety. Across the **sector,** the focus is on collective impact, coordination, shared resources, and information flow. **The output** will be a publicly-released report to summarize the shared understanding and outcomes*

What are the anticipated resource requirements for participation?

*A **Lead Planner/Point of Contact** to organize internal participation and provide consolidated feedback to feedback forms and surveys*

*~8 hours of **Exercise Participant** engagement (for up to twenty players per enterprise over two days)*

https://portal.h-isac.org/s/community-event?id=a1YVn000005Bd3B

OPERATION VITAL SIGNS
NATIONAL CYBERSECURITY EXERCISE FOR THE HEALTH SECTOR

Upcoming Webinars and Virtual Events

Clearwater's Monthly Cyber Briefing | 12pm – 1pm CT

- You are already enrolled. Next session August 6th
- Featuring Dave Bailey, Illiana Peters, Polsinelli & Robert Kantrowitz, Kirkland & Ellis

Beyond Responsible AI | 5-Week Summer Virtual Series | June 24 – July 22, 2026

Governing Healthcare in an Era of Intelligent Systems

Register Now ›

- Register here

OCR-Quality® Risk Analysis Working Lab 2026: Beginning August 12 @ 11:00 am CT

Quick single registration for five sessions. Hands on, interactive series to help healthcare organizations meet OCR's Security Risk Analysis requirement, reduce cyber risk, and prepare for heightened HIPAA Security Rule expectations

Register Now ›

- Register here

OCR-Quality® Risk Response Working Lab 2026: Beginning September 16 @ 11:00 am CT

Hands On, Interactive Series to Help You Drive an Efficient and Effective Risk Management Process

Register Now ›

- Register here

Clearwater

Upcoming In-Person Events

Learn more + book a meeting

Learn more + book a meeting

Clearwater

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/

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.