Fortified HEALTH SECURITY

2026 HORIZON REPORT

The State of Cybersecurity in Healthcare

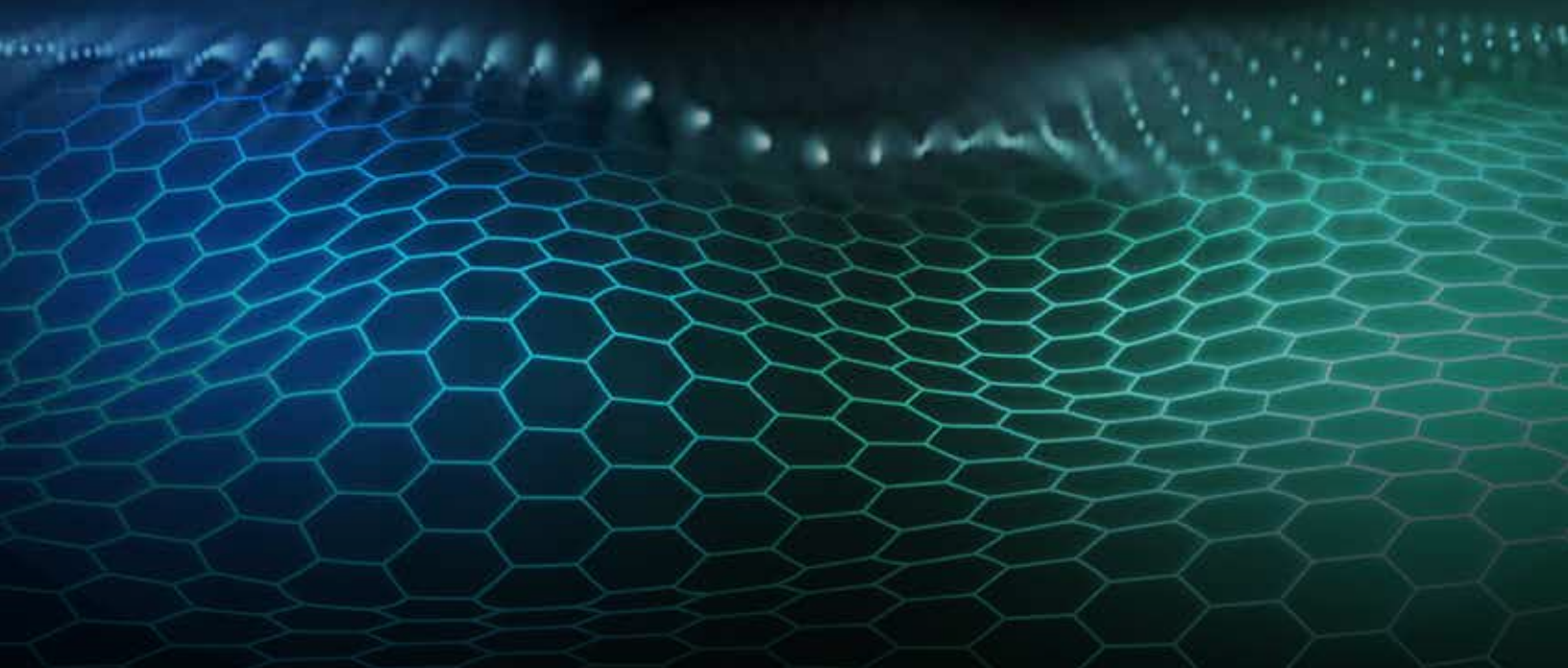


Table of Contents

03 **CEO Message:**
Relentless Momentum

04 **2025's Breach Landscape:**
A Year Defined by Variability and Rising Frequency

08 **What Breach Frequency Reveals About Cybersecurity Readiness**

12 **Leading Through the Breach:**
Inside Frederick Health's Ransomware Response

16 **Shadow AI in Healthcare:**
The Invisible Insider Threat

19 **Back to Basics:**
Why Continuous Cybersecurity Training Is Healthcare's Strongest Defense

22 **The Regulations Driving Healthcare Cybersecurity Forward**

26 **Beyond the Technology:**
Building Relentless Momentum Through Human-Centered Cybersecurity

28 **What We're Excited About:**
A Stronger, Smarter Year Ahead

30 **About the Contributors**

31 **About Fortified Health Security**

CEO MESSAGE

"Relentless Momentum"

As we head into the new year, many of us start to think about building healthier habits and stronger routines. I began my health journey last summer with a new commitment to work out more, and build strength, endurance, & consistency. But here's what I've realized: it doesn't get easier. The moment you achieve one level, the next challenge is already waiting. The weight gets heavier. The pace gets faster. The bar moves.

Threats don't pause, and innovation doesn't slow down, but that constant motion is what drives progress. The mission to protect patients and systems keeps moving forward because of people. Clinicians, engineers, analysts, and partners show up every day with expertise and resolve, solving complex problems and advancing what matters most: patient care.

At Fortified, we move forward together. We don't just react; we anticipate. We don't build inside a vacuum; we innovate solutions alongside our partners. Our Central Command platform is a prime example. Over the past year, we delivered new releases every month, along with key upgrades and new features shaped by honest client feedback.

Beyond technology, our momentum extended to strategic growth and connection. With the acquisition of Latitude, we strengthened our ability to serve healthcare organizations nationwide. And with the opening of the only healthcare cybersecurity Executive Briefing Center at our Nashville headquarters, we created a space where clients can experience innovation, collaboration, and cybersecurity leadership firsthand.

Real resilience isn't a one-time achievement. It's a daily commitment grounded in purpose, powered by people, and strengthened by partnership.

Relentless momentum.
It never stops. Neither do we.

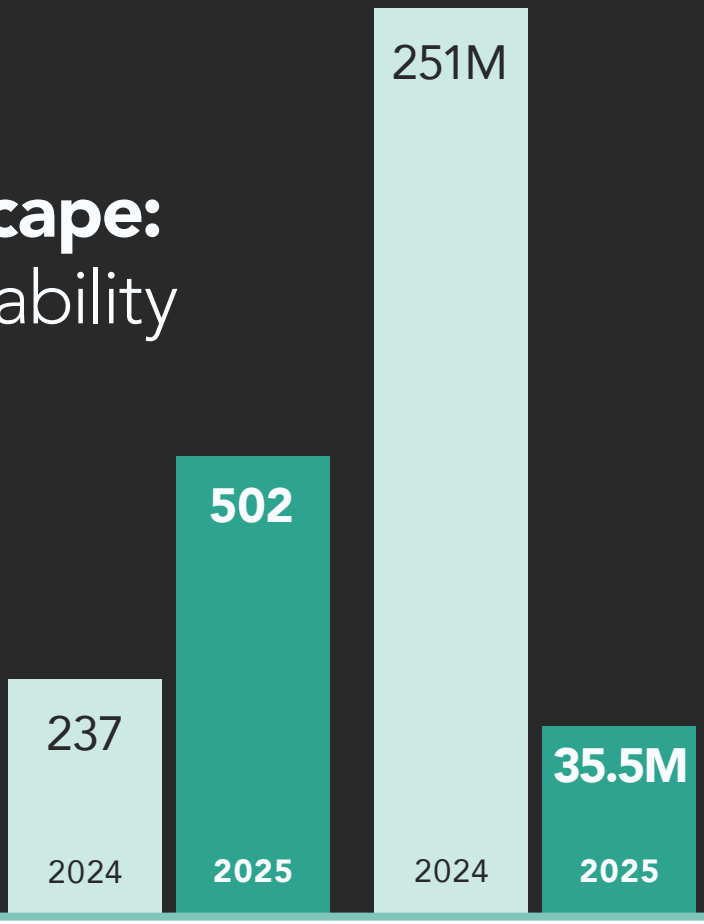
Warm regards,

Dan L. Dodson

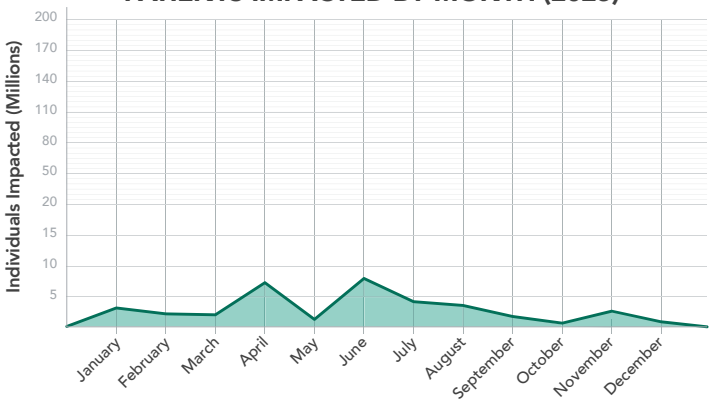
2025 ANNUAL REVIEW

2025's Breach Landscape: A Year Defined by Variability and Rising Frequency

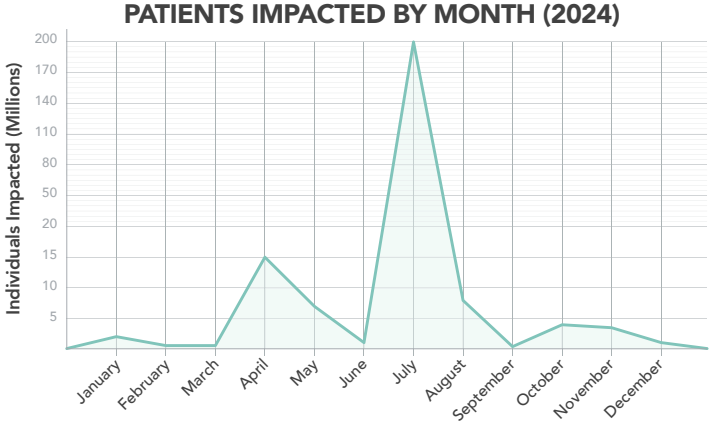
In 2025, the healthcare industry saw a transformation from the mega-breaches of 2024 (Change Healthcare) to more breaches, but less patient information impacted.



PATIENTS IMPACTED BY MONTH (2025)



PATIENTS IMPACTED BY MONTH (2024)

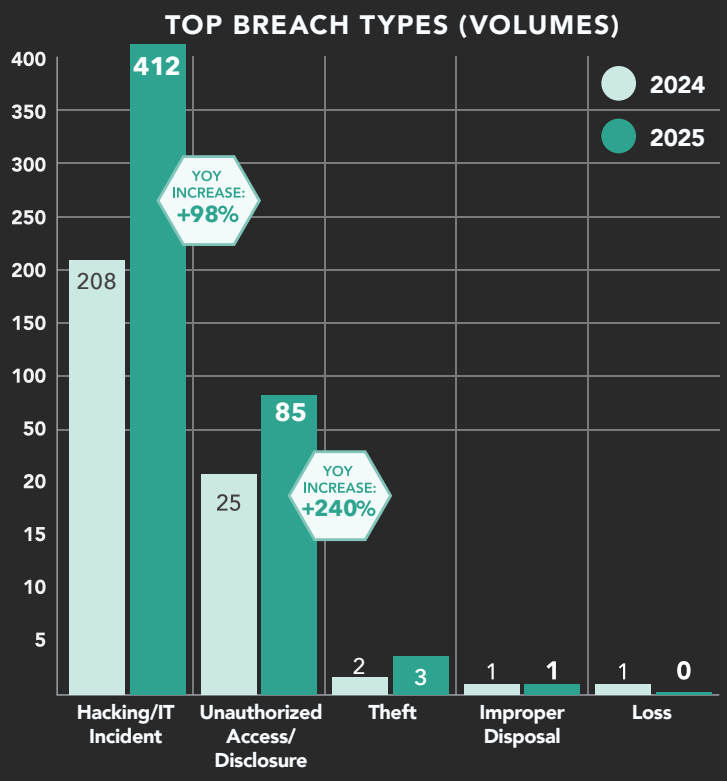


112% **Total breach counts in 2025 surpassed 2024 by roughly 112%.**

OCR data shows that total breach counts in 2025 surpassed 2024 by **approximately 112%**, yet the number of individuals affected remained far lower.[1] The healthcare sector is experiencing more frequent cyber events with smaller data footprints, driven largely by ransomware, identity compromise, and third-party weakness.

This represents progress in limiting breach size, but also signals a new phase of cyber risk, where operational resilience, response capacity and workforce sustainability matter as much as traditional data protection measures.

1 Data from the U.S. Department of Health and Human Services Office for Civil Rights January 2024 - December 2025



The Shift in Breach Types

Hacking and IT incidents continued to dominate in 2025 and grew faster than any other category. **Reported incidents more than doubled the previous year,** driven by:

- Exploitation of exposed servers, VPNs, and RDP
- A rise in credential theft and MFA-bypass activity
- Cascading compromises linked to vendors and third-party service providers

Unauthorized Access and Disclosure were the fastest-growing secondary category. Much of this increase stemmed from routine but consequential workforce errors: misdirected communications, inappropriate internal access, and early signs of Shadow AI risks where the adoption of tools occurred without adequate oversight or training.

Where Breaches Happened

Network servers remained the most common location for compromised data. But the most notable movement occurred in email-based breaches, which more than doubled year-over-year. This trend reflects growing exposure through phishing, credential misuse, and misdirected messages.

Paper records and EMR-related breaches also saw moderate growth, underscoring the continued vulnerability of workflows that remain partially manual or hybrid.

LOCATION	2024 BREACHES	2025 BREACHES
Network Server	174	305
Email	39	123
Paper/Films	6	21
Electronic Medical Record	5	20
Other	3	12
Desktop Computer	1	5
Laptop	2	2

What 2025 Revealed

The volatility and rising frequency of breaches mean healthcare is facing a threat environment that is less predictable, more distributed, and increasingly opportunistic. The absence of a single major event hid a more sinister threat: Attacks that come faster, hit more healthcare organizations, and strain teams through repetition rather than scale. Because of this, the healthcare industry's focus on defense and resilience has become essential.

Those organizations that maintained momentum in strengthening their cybersecurity programs (refining identity controls, tightening third-party governance, enhancing training, and maturing incident response) were better equipped to handle the year's rollercoaster ride.

Areas of Momentum

Here are some of the biggest areas of momentum we saw year-over-year according to Fortified Health Security's rolling **NIST Cybersecurity Framework (CSF) assessments:**

- **Awareness Training:** Six months after landing on our Mid-Year Horizon Report's "Continued Risk Area" list, Awareness Training has shown improvement year-over-year. This is a positive sign that organizations' cultures are changing, and cybersecurity is becoming more a part of the organizational DNA.
- **Detection Processes:** After not ranking among the top five momentum areas in the mid-year Horizon Report six months ago, detection processes have increased year-over-year. This growth reflects healthcare organizations improving visibility, formalizing detection and response workflows, leveraging outsourced support, and aligning more closely with regulatory expectations and resilience strategies.

> **Attacks that come faster, hit more healthcare organizations, and strain teams through repetition rather than scale.**

The Gaps

While we are seeing the impact of cybersecurity momentum, there are still gaps that healthcare organizations need to make more progress on, especially when it comes to Third-Party Risk Management and end-user awareness training.

TPRM

Fortified conducted polls in 2025 with healthcare leaders across the U.S. We asked about how confident healthcare leaders are with how their current third-party risk assessments align with the actual level of risk each vendor poses.

Only 4% of those surveyed were very confident, while 29% were not confident at all.

TPRM Alignment:

Q: How confident are you that your third-party risk assessments align with the actual level of risk each vendor poses?

Survey Results:

Training

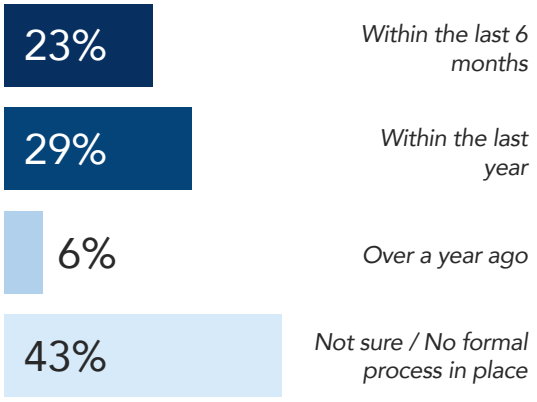
While our data shows awareness training is up, healthcare organizations still need to find the time to make policies to ensure every employee is trained in cybersecurity. Especially when we see the huge year-over-year increase in OCR data for Unauthorized Access and Disclosure stemming from workforce errors, meaning an email getting through or shadow AI coming into play.

When we asked healthcare leaders about their training protocols, here is what we discovered:

Testing the Basics:

Q: When was the last time your organization refreshed or retrained staff on foundational security practices like patching, access control, or least privilege?

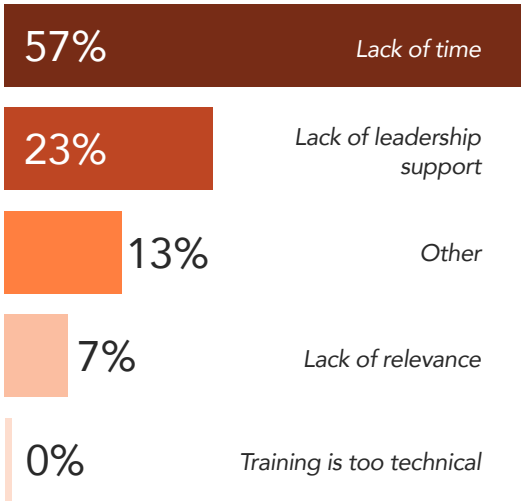
Survey Results:



Barriers to Training:

Q: What's the biggest barrier to effective cybersecurity training in your department?

Survey Results:



What Comes Next

The next challenge for healthcare organizations is to turn **volatility into visibility** and readiness before the next major breach hits. Resilience will depend on that same momentum, pushing defense strategies, operational discipline, and visibility further than before.

What Breach Frequency Reveals About Cybersecurity Readiness

The 2025 breach outlook paints a picture familiar to healthcare leaders: Breaches are more frequent but affect fewer patient records. The industry has shifted from major, headline events to a more taxing state of constant disruption.

More alerts. More investigations. More decisions under pressure. Less time to reset.

This shift matters. Because when breaches become routine, cybersecurity stops being a crisis problem and becomes an endurance problem. And endurance is not built on technology alone.

> **More alerts.**
> **More investigations.**
> **More decisions under pressure.**
> **Less time to reset.**

6% OF HEALTHCARE ORGANIZATIONS

say they are very confident in their ability to detect, contain, and recover from a cyber incident.

Why the "Single Fix" Mentality Falls Short

Healthcare organizations are not standing still.

Our **2025 survey** shows most have added or expanded cybersecurity capabilities over the past year. But only a small number have redesigned their programs in a meaningful way. Progress is happening carefully, pragmatically, and under real financial pressure.

In many cases, that progress takes a familiar form. When budget becomes available, another tool is added. When a new risk emerges, another service is layered in. Over time, technology stacks grow incrementally, often without the integration, staffing, or process needed to fully operationalize what's already in place.

That kind of momentum is understandable. But momentum without alignment eventually creates friction.

When something breaks, the instinct is to fix that thing. A new tool. A new service. A new assessment. And sometimes, that's the right move.

But healthcare cybersecurity doesn't fail in isolation. It fails where people, process, technology, and budget fall out of sync.

2025 SURVEY:

The Human Reality Behind Cybersecurity Readiness

Insights from Fortified's 2025 Healthcare Cybersecurity Survey

- **Only 6% of healthcare organizations** say they are very confident in their ability to detect, contain, and recover from a cyber incident.
- Most leaders report being somewhat confident, signaling progress without full trust in speed or consistency under pressure.
- Cybersecurity progress is largely incremental, with organizations adding capabilities carefully rather than redesigning programs.
- Long-tenured staff carry critical institutional knowledge, while turnover and burnout continue to strain teams.
- Leaders consistently cite program structure and trusted partners as essential to sustaining readiness when internal capacity is limited.

PEOPLE:

Designing Programs for Turnover and Reality

Cybersecurity programs rise and fall with people.

Experience matters. Institutional knowledge matters. Across healthcare, many cybersecurity teams rely on long-tenured employees who grew up inside the organization. These individuals bring deep system knowledge, strong community ties, and a lasting commitment to patient care. These "lifers" form the backbone of many programs.

At the same time, turnover is real. Cybersecurity talent can often earn more outside of healthcare, and some roles turn over quickly. Hiring is hard, burnout is common, and churn is not a leadership failure. It is a structural reality of the industry. Programs designed around perfect staffing conditions rarely survive contact with reality.

That reality shows up in confidence levels. Only a small percentage of healthcare organizations say they are very confident in their ability to detect, contain, and recover from an incident. That lack of confidence is not a failure of effort. It is a signal that teams are being asked to carry too much without enough structural support.

Strong programs do not assume stability. They assume change and plan for it by strengthening the people who stay, preserving institutional knowledge, and ensuring that capability does not disappear when individuals do.

PROCESS:

Turning Lessons Learned into Muscle Memory

Technology gets attention.
Process determines outcomes.

Some organizations revisit cybersecurity policies continuously, embedding them into daily operations. Others rely on periodic updates tied to audits or compliance cycles. The difference is not paperwork. It is readiness.

Recent breach patterns show that repetition wears teams down faster than scale. When organizations do not operationalize lessons learned, they fight the same fires again and again.

> **Technology gets attention. Process determines outcomes.**

TECHNOLOGY:

Operational Value Beats Feature Depth

Technology stacks across healthcare continue to grow. Identity platforms, detection tools, and monitoring solutions are now common. What is missing is not capability. It is clarity.

Speed of recovery depends on coordination, visibility, and trusted partnerships. Tools reduce risk only when they can be fully operationalized and sustained over time.

BUDGET:

Protecting Patients Under Financial Pressure

Every cybersecurity decision in healthcare is made under financial pressure. Each dollar invested in security is a dollar not spent at the bedside.

That reality is shaping priorities for the year ahead. Leaders are focusing on incident response readiness, data protection, zero trust, and third-party risk management not because they are trendy, but because they reduce real risk in real environments.

The question healthcare leaders are asking is no longer what to add, but how to protect more with what already exists.

> **Each dollar invested in security is a dollar not spent at the bedside.**

THE 2026 IMPERATIVE:

Program Thinking Over Product Thinking

The healthcare organizations best positioned for the future are not the ones with the biggest budgets or the most tools. They are the ones that think in programs, not products. They plan for turnover. They practice response. They optimize before they add. They learn from peers. They treat readiness as a habit. Healthcare cybersecurity momentum matters. But readiness is what carries organizations through the next disruption and the one after that.

Leading Through the Breach: Inside Frederick Health's Ransomware Response

By the Fortified Threat Services Team

Frederick Health Medical Group experienced a ransomware attack in early 2025 that affected more than 900,000 patient records and slowed operations for weeks. The headlines focused on patient notifications and system outages. But for security leaders across healthcare, **the greater lesson lies in what happened behind the scenes:** the decisions, reactions, and lessons that define how ready an organization really is **when a crisis hits.**

Frederick Health
MEDICAL GROUP

4000
EMPLOYEES

25
LOCATIONS

Frederick Health Breach Timeline

JANUARY 27, 2025

THREAT DETECTED

FHH's IT team detected unusual network activity, prompting an immediate emergency shutdown of critical systems to contain the threat. Systems taken offline, ambulances diverted, ED shutdown (Mini-disaster designation by Maryland Institute for EMS systems.)

PATIENTS NOTIFIED

JANUARY 28, 2025

With digital systems offline, the hospital activated downtime procedures, including a transition to paper-based record-keeping for patient care.

FEBRUARY 6, 2025

Cybersecurity experts confirmed that ransomware was the cause of the disruption. Law enforcement agencies, including the FBI, were notified to assist with the investigation.

MARCH 28, 2025

Incident reported to the U.S. Department of Health and Human Services noting 934,326 patients impacted.

Red Team (Threat Operations)

The offensive team that simulates real-world attackers (ethical hackers) to find and exploit vulnerabilities in an organization's defense.

Blue Team (Threat Defense)

The defensive team that protects systems by detecting, responding to, and preventing these attacks in real-time.

Fortified's **Threat Operations (Red Team)** and **Threat Defense (Blue Team)** leaders take us through each stage of the incident response cycle as it relates to the Frederick Health breach, revealing how healthcare organizations can shorten recovery timelines, avoid early missteps, and build resilience before the next breach makes the news.

Why Peer Breach Experiences Matter

Based on 2025 Fortified Health Security survey results from U.S. healthcare organizations

- **Over one-third of organizations** changed their cybersecurity approach after learning from another organization's cyber event.
- **Only 6%** of healthcare organizations report being very confident in their ability to detect, contain, and recover quickly.
- **Incident response readiness** is the top area healthcare leaders say they want to accelerate in 2026.

STAGE 01

PREPARATION:

Knowing Where You're Weak

Frederick Health's event began on January 27, when the health system noticed unusual network activity and initiated an emergency shutdown. Within days, the FBI confirmed a ransomware attack.

Q: Before this attack, what defenses or drills could have made the biggest difference?

Red Team *(TJ Ramsey)*

Many healthcare organizations still view preparation as a compliance checkbox instead of a readiness discipline. It's not just about finding gaps; it's about practicing what you'll do when those gaps are exploited. Pen testing and tabletop drills are the difference between guessing and knowing.

Blue Team *(Jake Bice)*

Readiness hinges on visibility. Preparation isn't just about tools. It's about understanding where you're weak and closing the loop between security, IT, and operations before an alert ever fires.

What could have helped

Continuous vulnerability testing, network segmentation, and rehearsed communication between clinical and IT staff could have slowed lateral movement and clarified decision-making in the first hours of the attack.

> **When it happens, it's we, not me. Everyone, from the SOC to the nurses' station, is fighting the same fight.**

TJ Ramsey // Senior Director, Threat Operations

STAGE 02

DETECTION & CONTAINMENT:

Seconds Matter

In Frederick Health's case, "unusual network activity" was the first clue. By then, ransomware was already in motion.

Q: What would you look for to confirm "unusual activity"?

Blue Team *(Jake Bice)*

Endpoints are where ransomware lives. If you're still relying on antivirus instead of behavioral EDR, you're already behind. Modern EDR gives you real-time telemetry, identity monitoring, and the ability to hunt across every device before encryption spreads.

Red Team *(TJ Ramsey)*

There also needs to be an emphasis on the importance of tuned logging and alerting well before an event. If your firewall keeps getting password-sprayed, that's your warning shot. Move fast before the breach, not after.

Blue Team *(Jake Bice)*

You can't stop the bleeding if you don't know what organs you're protecting. You have to know what's vital to keeping the organization going. Asset inventories and segmentation plans decide whether you can act decisively or just react.

What could have helped

Comprehensive asset mapping and layered detection tools to isolate infected systems quickly without halting patient-critical applications.

STAGE 03

ERADICATION & RECOVERY:

Acting Fast Without Acting Emotional

On February 6, 2025, Cybersecurity experts confirmed that ransomware was the cause of the disruption.

Q: Once ransomware is confirmed, what's step one?

Red Team *(TJ Ramsey)*

Once ransomware is confirmed, the first step is assessing impact: which departments are down, where backups live, and who has authority to make the next call. Establish your command center, activate your incident response playbook, and get your partners on the phone. Every hour matters, but panic is expensive.

Blue Team *(Jake Bice)*

Yes, emotional decisions can worsen damage. The most common recovery mistake is acting too fast, shutting everything down, re-imaging without preserving evidence, or trusting a backup that's already infected. Recovery has to be methodical, even under pressure.

What could have helped

A current, tested incident response plan stored in a mobile-accessible platform would have accelerated decision-making, preserved forensic evidence, and coordinated external responders more efficiently.

STAGE 04

NOTIFICATION & LESSONS LEARNED:

The Long Tail of Recovery

Frederick's patient notifications went out roughly two months after the breach; a timeline that, while appearing slow to the public, is actually swift in regulatory terms.

Q: Why might patient notification take two months?

Red Team *(TJ Ramsey)*

The process involves legal and forensic steps most outsiders never see. Hospitals can't notify until they know which records were exposed. That means e-discovery, deduplication, and validation of every name, every file. So, in this case, two months is much faster than we've seen in most ransomware situations.

Blue Team *(Jake Bice)*

For hospitals, the challenge extends beyond compliance to trust. You only get one chance to tell your community the truth. How and when you communicate defines your recovery as much as how fast your systems come back online.

What could have helped

Pre-approved notification templates and legal coordination workflows so leaders can focus on patients, not paperwork.

THE TAKEAWAY:

Readiness Is Culture

The Frederick Health case reinforced a hard truth: ransomware is not a technology problem alone; it's also a readiness problem that demands collaboration across every layer of a healthcare organization, not just IT.

Red Team *(TJ Ramsey)*

When it happens, it's we, not me. Everyone, from the SOC to the nurses' station, is fighting the same fight.

Blue Team *(Jake Bice)*

No one has an unlimited budget. The best defense is knowing your limits, building partnerships, and investing in the basics that buy you time when every second counts.

Shadow AI in Healthcare: The Invisible Insider Threat

By Preston Duren // *Vice President of Threat Services, Fortified Health Security*

Artificial intelligence is no longer an emerging technology; it is part of the daily routines of the healthcare ecosystem. Clinicians, IT teams, and administrators are using transcription tools and AI summaries for greater efficiency and improved patient outcomes. But innovations like this come with significant risk for healthcare organizations.

Shadow AI, the unsanctioned use of artificial intelligence tools outside of an organization's approved governance framework, poses one of the most immediate and underestimated threats facing healthcare today.

Shadow AI isn't about bad actors; it's about smart people trying to work smarter. But without governance, good intentions can still cause serious harm.

> **Shadow AI isn't about bad actors; it's about smart people trying to work smarter. But without governance, good intentions can still cause serious harm.**

The Rise of Shadow AI

Across the industry, I see clinicians and staff turning to consumer-grade tools such as ChatGPT or transcription applications to make their jobs easier. These tools provide real value. When used without organizational vetting or HIPAA compliance, though, they can introduce risk on a scale that most leaders underestimate.

Each upload, transcription, or query may be sending sensitive data into external environments that cannot be monitored or controlled.

The reality is that the adoption of AI tools is happening faster than healthcare organizations can write policies. Across clinical, administrative, and technical roles, employees are embracing AI to work smarter, but most organizations are still scrambling to catch up with guardrails.

This widening gap between adoption and oversight has created a visibility problem that leaders cannot ignore.

> **The adoption of AI tools is happening faster than healthcare organizations can write policies.**

When Productivity Becomes a Blind Spot

Shadow AI may be the biggest data exfiltration risk we've ever faced because it doesn't look like an attack; it looks like productivity. Clinicians often assume that if they are using a helpful tool, the organization's IT systems will automatically ensure compliance. But when entering data into an external AI platform, it effectively leaves the organization's control.

This is what makes shadow AI so insidious. Anyone using shadow AI can unknowingly exfiltrate sensitive information to third-party systems where it becomes part of external models. Shadow AI doesn't just leak data; it donates it to someone else's model. Once uploaded, it cannot be retrieved or deleted.

> **Shadow AI may be the biggest data exfiltration risk we've ever faced.**

Beyond privacy risks, AI-generated content also introduces issues of accuracy. When large language models hallucinate, they can produce incorrect but highly convincing information that finds its way into patient records, coding, or treatment decisions.

Why Blocking AI is Not the Solution

Healthcare organizations may have a knee-jerk reaction to block AI tools altogether, but that approach is impractical and counterproductive. If an organization restricts access, users will move to personal devices. The more sustainable solution is to make safe AI usage easier than unsafe usage. If you want people to follow processes, make processes easy to follow. When governance frameworks are too rigid, they fail to keep pace with innovation.

Organizations must provide approved, accessible, and compliant alternatives that enable employees to benefit from AI without introducing unnecessary risk. Embedding trusted AI capabilities within established, HIPAA-compliant systems ensures that clinicians can achieve efficiency and accuracy without exposing data. Major electronic health record vendors are already integrating AI directly into their secure platforms, a model that represents the future of responsible adoption.

Building Visibility, Governance, and Collaboration

In cybersecurity, we can only protect what we can see. The challenge with Shadow AI is that AI-related behavior looks like ordinary activity, making detection difficult. Healthcare organizations must establish visibility frameworks that identify when and where employees are using AI tools, detect large or unusual data uploads, and educate staff on safe prompting techniques that minimize exposure.

Healthcare organizations can't address this on their own. It requires alignment across leadership, compliance, IT, and cybersecurity teams. Leaders must treat AI governance as a core business initiative driven by executive sponsorship. When organizations create a culture that promotes awareness, transparency, and shared accountability, they are far more likely to achieve the balance between innovation and safety.

Every clinician and staff member now has the potential to become an unintentional insider threat. It's not about negligence; it's just a result of how accessible AI has become. Recognizing that is critical to developing realistic safeguards that focus on enablement rather than punishment.

> **If you want people to follow processes, make processes easy to follow.**

A Proactive Path Forward

Managed security providers can play an essential role in helping healthcare organizations address this visibility gap and build AI governance strategies that align with compliance requirements while enabling innovation. Advisory services, monitoring enhancements, and updated risk assessments can help healthcare organizations get a better understanding and manage AI-related exposure.

Key priorities include:

- Defining AI governance policies and acceptable use thresholds
- Integrating AI-specific traffic monitoring into SOC and EDR platforms
- Incorporating AI risk into enterprise risk assessments and NIST-aligned frameworks

AI adoption in healthcare is inevitable. The question is whether leaders will adopt it with visibility and control, or reactively, after an incident has exposed weaknesses. By acting now to formalize AI governance, healthcare leaders can turn what is currently a visibility challenge into a strategic advantage.

AI adoption in healthcare is inevitable.

Back to Basics: Why Continuous Cybersecurity Training Is Healthcare's Strongest Defense

By Jason Stewart // *vCISO Manager, Fortified Health Security*

Did you know that cybercrime is the third largest GDP in the world?

Got your attention? Good, because that fact is precisely why healthcare organizations must get back to the basics and embrace education as the foundation of their cybersecurity strategy.

For all the complexity surrounding cybersecurity, the most consistent factor behind a breach is still human error. Training is not a one-and-done task or an annual compliance checkbox. Training is the single most important investment in building a defensible cybersecurity posture.

> **Training is the single most important investment in building a defensible cybersecurity posture.**

Moving Targets and Moving Minds

Cybersecurity is an ever-shifting target. Threat actors evolve faster than most organizations can react, adapting new technologies and social engineering tactics that exploit human nature. As healthcare staff face new challenges every month, from phishing campaigns that mimic internal memos to deepfake calls requesting MFA resets, a once-a-year awareness module is no longer enough.

Continuous education that is short, frequent, and relevant keeps people alert and aware. Like hand hygiene or patient safety checks, cybersecurity must become a living practice built into everyday workflows.

Mandates, Momentum, and the Culture Shift

Across the country, regulations are beginning to catch up. Texas and New York now require cybersecurity awareness training for anyone using a computer for more than 25 percent of their workday. But culture, not compliance, is what creates real change.

The organizations doing this right do not just require training. They celebrate it. They make cybersecurity part of their DNA. Incentives, recognition, and leadership engagement all play a role. When executive leaders champion training as a business imperative, participation skyrockets. When leaders recognize staff for spotting real phishing attempts, they become ambassadors for security awareness.

The best programs track adoption rates, maintain accountability, and tie completion to measurable outcomes. Some even link training performance to annual reviews. Others encourage friendly competition between departments. The result is not fear, it is pride. The culture becomes one where everyone understands that protecting patient data is everyone's job.

CULTURE DRIVERS THAT WORK:

- **Leadership messaging** and visible participation
- **Incentives** tied to completion and performance
- **Regular recognition** of individuals or departments
- **Ongoing communication** that keeps security top of mind

Fundamentals Are Never Optional

The fundamentals never change. It always includes phishing awareness, password management, access control, and basic digital hygiene. What changes are the tactics used against them? As artificial intelligence makes attacks more convincing and personal, the ability to think critically and pause before clicking is more valuable than ever.

One of my mentors once said that the size of your security team should be "everyone who works here." I believe that wholeheartedly. Every nurse, technician, and billing coordinator plays a role in protecting the organization. They are the first line of defense, and education gives them the tools to recognize when something does not look right.

CYBERSECURITY FUNDAMENTALS EVERY EMPLOYEE SHOULD KNOW:

- **Recognize phishing** red flags
- **Verify sender identity** before clicking or responding
- **Protect credentials** and report MFA reset requests
- **Understand the process** for reporting incidents quickly

Building Relentless Momentum

At Fortified, we talk often about relentless momentum. That means continuous improvement and never assuming you are safe because you passed last year's phishing test. It means setting ambitious goals, like 90 percent training adoption, and backing those goals with leadership support, consistent communication, and creative incentives.

When people are excited to learn and proud to protect their organization, you begin to see cybersecurity as a shared mission, not an obligation. The result is a workforce that not only avoids being a risk but actively strengthens your defense posture.

HOW TO BUILD MOMENTUM:

- **Set measurable** adoption goals
- **Secure executive** sponsorship
- **Use incentives** to boost engagement
- **Recognize top performers** and share success stories

> **If your people do not know how to recognize, resist, or report a threat, it only takes one email, and one click to cause catastrophic damage.**

The Most Important Investment

The number one investment any organization can make in cybersecurity is education. You can purchase every tool on the market, but if your people do not know how to recognize, resist, or report a threat, it only takes one email, and one click to cause catastrophic damage.

We prepare for when, not if, a breach happens. And only when your entire workforce understands its role and feels empowered to act, you dramatically reduce the odds of becoming the next headline. Building that kind of readiness starts with the basics, and it never stops.

The Regulations Driving Healthcare Cybersecurity Forward

By Russell Teague // CISO, Fortified Health Security

For years, healthcare cybersecurity has asked for clarity, and in 2026 we finally have some.

But it comes with a challenge.

Federal focus has shifted from crisis response to structural reform. Two initiatives now stand to reshape how hospitals, especially rural and regional systems, fund and secure their digital operations: the Rural Health Transformation (RHT) Program and the Interoperability and Prior Authorization Final Rule (CMS-0057-F).

These programs share a single thread: modernization. But modernization without cybersecurity isn't progress; it's exposure.

While the funding is for technical advances, the outcome is cybersecurity resilience, which ultimately means protecting patients.

The Rural Health Transformation Grant

The new RHT Program, authorized under the Consolidated Appropriations Act of 2025 and launched by CMS in late 2025, directs $50 billion over five years to help states strengthen rural healthcare delivery.[1] Unlike past grant cycles, cybersecurity is explicitly part of the investment strategy. Through the Rural Transformation Program, states can fund "technical assistance, software, and hardware for significant information technology advances designed to improve cybersecurity capability development."[2] While the funding is for technical advances, the outcome is cybersecurity resilience, which ultimately means protecting patients.

As I shared in my commentary for Health IT Answers, this program represents both opportunity and risk. The opportunity lies in long-overdue investment for rural infrastructure. The risk lies in speed. Funding cycles are tight. Applications were due by late 2025, and many organizations are still struggling with limited cybersecurity maturity. If we move too fast without governance, we risk building technical debt and new vulnerabilities into the very systems meant to expand access.

50% of organizations update cybersecurity policies continuously. The remaining 50% still rely on periodic or compliance-driven policy updates.

2025 Fortified Health Security survey results from U.S. Healthcare Organizations.

Security leaders should approach this grant strategically:

- Advocate for funding allocations that include modernization of endpoint protection, identity management, and third-party oversight.
- Frame cybersecurity not as overhead, but as the foundation of digital care access.
- Pair every capital investment with a maintenance and sustainability plan to ensure that security posture does not decay after spending grant dollars.
- Build defensible architectures that align with broader telehealth and data-sharing objectives.

It's more than compliance; it's a rare chance for rural facilities to close long-standing security gaps and raise their baseline posture while avoiding the hidden risks of rushing modernization.

1 *www.cms.gov/priorities/rural-health-transformation-rht-program/overview*

2 *www.healthitanswers.net/rural-health-transformation-a-50-billion-opportunity-with-tight-deadlines-and-hidden-risks/*

Security & interoperability can no longer be **separate conversations.**

The Interoperability Mandate

On the other end of the spectrum, the CMS Interoperability and Prior Authorization Final Rule takes effect in January 2026.[1] It requires payers and providers to adopt standardized FHIR APIs and implement real-time data sharing across networks.

The benefit is clinical efficiency; the risk is exponential exposure. Every new API connection, patient app, and data exchange creates a potential breach pathway. Security and interoperability can no longer be separate conversations.

They are two sides of the same mission: Safe, connected care.

Healthcare organizations should:

- Map and monitor every data-sharing endpoint.
- Align with the new Health Data, Technology, and Interoperability (HTI-1) rule timelines.[2]
- Require interoperability-compliant vendors to prove encryption, audit logging, and identity verification readiness.

The result will go beyond compliance and include confidence, knowing your system is secure as data moves across the care continuum.

1 www.cms.gov/cms-interoperability-and-prior-authorization-final-rule-cms-0057-f

2 www.healthit.gov/topic/laws-regulation-and-policy/health-data-technology-and-interoperability-hti-1-final-rule

The HIPAA Security Rule Update

Another long-anticipated regulatory shift could happen this year.

On January 6, 2025, HHS and OCR published the Notice of Proposed Rulemaking (NPRM) titled *"HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information."*

As of now, OCR has kept the rule on its official regulatory agenda with a projected finalization date of May 2026. If it's finalized, this would be the biggest update to the HIPAA Security Rule in twenty years, modernizing requirements around risk analysis, authentication, vendor oversight, and technical safeguards while better aligning regulatory expectations with today's threat landscape.

> **The HIPAA Security Rule update would modernize requirements around risk analysis, authentication, vendor oversight, and technical safeguards.**

MC2 v2 gives providers a practical tool for holding vendors accountable and aligning security obligations across the care ecosystem.

The Role of HSCC's Model Contract Language (MC2 v2)

To support this regulatory momentum, the Health Sector Coordinating Council's (HSCC) Model Contract Language for MedTech Cybersecurity (MC2 v2) adds a critical layer of clarity for healthcare organizations working with medical device manufacturers.[3]

Updated in November 2025, MC2 v2 offers "pre-negotiated" cybersecurity terms that eliminate long-standing ambiguity around responsibility and risk. **It establishes shared expectations for:**

- Secure-by-design development
- Vulnerability disclosure
- Patch validation
- Responsible data handling
- Supplier transparency
- Lifecycle management of devices

The framework also includes a maturity roadmap that helps organizations phase in requirements over time, ensuring that capabilities such as encryption, secure authentication, OS accountability, remote access controls, and SBOM transparency evolve in step with broader industry standards. In a year defined by regulatory acceleration, MC2 v2 gives providers a practical tool for holding vendors accountable and aligning security obligations across the care ecosystem.

3 *https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/*

Rural networks gaining new technology need governance.

Urban systems connecting to new APIs *need monitoring.*

Converging Priorities

Together, the RHT Program and interoperability mandates define healthcare's 2026 trajectory: expand access and ensure data fluidity. But both demand something else: A renewed cybersecurity discipline.

Rural networks gaining new technology need governance. Urban systems connecting to new APIs need monitoring. Every provider in between needs leadership that understands the intersection of security, regulation, and patient safety.

Lead the Way Forward

As CISOs, you can't treat these developments as bureaucratic checkboxes. These are signals of a maturing industry finally aligning policy with purpose thanks to your hard work. Now, your opportunity is to turn regulatory momentum into measurable resilience.

You can't afford to wait for another directive or funding round. The path is here, and the timing is now.

Beyond Technology: Building Momentum Through Human-Centered Cybersecurity

By Dr. Zafar Chaudry, MD, MS, MIS, MBA, CHCIO, CDH-E, SVP // *Chief Digital Officer & Chief AI and Information Officer at Seattle Children's*

In healthcare, progress in cybersecurity doesn't come from buying the newest tool or adding another layer of technology. It comes from **understanding people, processes, and purpose.** Technology is only the enabler, not the solution itself.

For years, I've said that it's never about the technology; it's the people and the process first. Sustainable cybersecurity requires aligning defense strategies with how care is actually delivered. When a clinician logs in, when a researcher travels, when a nurse accesses patient data at 2 a.m., those are the real moments where protection must live.

Seeing Security Through a Human Lens

In pediatric healthcare, we serve the most vulnerable population imaginable. That responsibility demands that our cybersecurity approach never loses sight of the human impact behind every alert, patch, or policy. The question I often ask my team is simple: Who are we serving? The answer is always patients, not IT, not compliance metrics, not technology stacks.

That clarity drives how we benchmark partners, select tools, and measure outcomes. Every decision has to connect back to enabling clinicians to care for patients safely. That means designing systems that support their workflow instead of slowing them down, and building processes that anticipate, not just react to, human behavior.

From Visibility to Actionable Insight

Technology should enhance situational awareness, not overwhelm it. When cybersecurity programs evolve beyond dashboards and alerts, they empower leaders to act with purpose. For example, gaining real-time visibility into user behavior, whether remote work trends or travel-based access patterns, enables proactive education, access control, and reinforcement of patient safety.

> Who are we serving? **The answer is always patients.**

> **Data without context is noise.**

That's where process design and human factors intersect. Data without context is noise. Data translated into insight becomes a force multiplier for decision-making across clinical, operational, and security teams.

Culture Is the Core of Cyber Resilience

No cybersecurity program succeeds in isolation. Its strength is rooted in culture, in how people collaborate, share responsibility, and adapt to change. At Seattle Children's, our teams know that cybersecurity isn't something IT "does" to the organization; it's something we all uphold together.

That culture extends beyond our walls to our partners and peers across healthcare. I often describe vendor relationships as marriages. There will be tough times and disagreements, but mutual trust, communication, and a shared mission to protect patients will help them thrive.

Relentless Momentum Means Continuous Learning

Relentless momentum in cybersecurity doesn't come from speed; it comes from discipline. It's about continuous learning and adapting. It's about reinforcing the fundamentals: training people, refining processes, and making security decisions that align with the clinical realities of healthcare.

When we focus on people and purpose first, technology naturally follows. And when we build a cybersecurity program around how humans actually work, it stops being a barrier to care and becomes an enabler of it.

What We're Excited About:
A Stronger, Smarter Year Ahead

The New Year brings new challenges in healthcare cybersecurity, but it also brings exciting momentum. Our industry is advancing through innovation, collaboration, and a renewed focus on resilience. These bright spots remind us that progress is not only possible; it's happening.

Here are six things Fortified is most looking forward to in the year ahead.

01

AI That Works for Defenders, Not Against Them

2026 is shaping up to be the year AI matures on our terms. The focus is shifting away from hype and toward practical applications that truly empower cybersecurity teams. We're seeing more AI-driven triage that reduces alert fatigue, LLM copilots that stay inside the firewall, and governed AI use in SOCs and IR playbooks. These tools emphasize explainability, accountability, and human augmentation, helping analysts move faster and smarter.

02

Momentum in Medical IoT Security

More than half of medical IoT devices are still vulnerable to serious attacks, but that's changing. New frameworks and tools are helping healthcare organizations segment, monitor, and patch connected devices in real time. In 2026, medical IoT security is maturing from awareness to action, especially in critical care environments where safety can't wait.

03

Zero Trust Becomes the Standard, Not the Goal

Healthcare systems are rapidly adopting Zero Trust Architectures and network segmentation as core strategies for multicloud and IoT environments. These approaches enforce continuous trust validation, least-privilege access, and real-time inspection of users, apps, and devices. Even at partial implementation, Zero Trust is reducing threat surfaces and building long-term resilience.

04

Cybersecurity Takes the Lead in M&A

Mergers and acquisitions continue to reshape healthcare, but each integration brings new risk. In 2026, cybersecurity is finally being treated as a strategic pillar of M&A, not an afterthought. Organizations are incorporating SASE frameworks and threat management processes directly into integration plans, ensuring that growth and security advance together.

For 2026, healthcare leaders are most optimistic about: **leadership attention, cross-industry collaboration, and AI-driven security innovation.**

2025 Fortified Health Security survey results from U.S. Healthcare Organizations.

05

Collaboration Across Policy, People, and Technology

The most inspiring change isn't just technological; it's cultural. Healthcare providers, regulators, and innovators are working together like never before to strengthen resilience and patient safety. One example we saw of this in 2025, was the new Healthcare and Public Health Sector Coordinating Council (HSCC) Policy Recommendations, which was the result of collaboration across more than 470 healthcare providers, payers, med-tech and health-IT companies, and government agencies. This collaboration is shaping a more connected, trusted, and proactive cybersecurity ecosystem across the industry.

06

Smarter, More Secure Digital Innovation

Digital innovation remains one of healthcare's greatest opportunities for progress. In 2026, that innovation is becoming more secure by design, powered by AI-driven threat detection, trusted data-sharing frameworks, and stronger alignment between IT and clinical operations. It's proof that modernization and security can advance together.

About the Contributors

Dan L. Dodson

CEO, Fortified Health Security

As the CEO of Fortified Health Security, Dan Dodson brings over 17 years of experience leading healthcare and insurance organizations. As a recognized thought leader in healthcare cybersecurity, Dan is a frequent speaker at industry events and conferences including CHIME, HIMSS, and HIT Summits. His insights and data-driven expertise in cybersecurity, data privacy, risk management, and threat mitigation are regularly featured in popular media and trade publications such as Forbes, Becker's Hospital Review, and Healthcare Business Today.

William Crank

COO, Fortified Health Security

William serves as COO of Fortified Health Security. For more than 25 years, he's driven the successful execution of cybersecurity strategies and tactics for the healthcare industry, including managing the Information Security Risk Management (ISRM) team at Hospital Corporation of America (HCA) and serving as Chief Information Security Officer (CISO) at MEDHOST.

Russell Teague

Chief Information Security Officer, Fortified Health Security

Russell Teague is a healthcare cybersecurity strategist with nearly three decades of experience advising healthcare organizations across complex environments. A U.S. Army Intelligence veteran, he brings a mission-driven, risk-informed approach to cybersecurity leadership, has consulted with the White House on national healthcare cybersecurity efforts, and is a frequent speaker at HIMSS, VIVE, HSCC, Health Connect Partners, and executive leadership events.

Dr. Zafar Chaudry, MD, MS, MIS, MBA, CHCIO, CDH-E

Senior Vice President, Chief Digital, Chief AI & Chief Information Officer at Seattle Children's

A visionary healthcare leader with over three decades of international experience, Dr. Zafar Chaudry is the driving force behind the digital and AI transformation at Seattle Children's. As Senior Vice President and Chief Digital, AI, and Information Officer, he spearheads initiatives that leverage cutting-edge technology to empower clinicians and ensure the delivery of exceptional, safe patient care.

Prior to joining Seattle Children's in November 2017, Dr. Chaudry served as CIO at several prominent institutions, including Cambridge University Hospitals and Liverpool Women's and Alder Hey Children's Hospitals in the U.K. He also previously held the role of Global Research Director at Gartner.

Jason Myers

Vice President, Advisory Services Operations, Fortified Health Security

Jason Myers is a seasoned technology executive with a proven track record of driving business growth. He joined Fortified in 2023 as the Vice President of Process Improvement and Globalization, where he was responsible for driving operational excellence and expanding the company's global footprint. Prior to joining Fortified, Jason spent several years at Amazon, where he led the Operational Technology Solutions (OTS) Centralized Services organization.

Preston Duren

VP of Threat Defense Services, Fortified Health Security

Preston Duren brings more than 16 years of IT/security expertise to his role as VP of Threat Defense Services at Fortified. His experience spans threat and vulnerability management, security engineering, security program development, digital forensics, and SOC.

T.J. Ramsey

Senior Director, Threat Operations, Fortified Health Security

T.J. Ramsey is a seasoned IT security professional with nearly 20 years of experience focused on healthcare and defense intelligence. He served as a U.S. Army Military Intelligence Analyst for the Department of Defense and held security roles at Obsidian Solution Group and SAIC/Leidos.

Jake Bice

Director, Threat Services, Fortified Health Security

Jake Bice is responsible for the strategic oversight of the Security Operations Center, assessing and resolving client needs, training teams, and refining the processes that underpin service delivery to clients. Jake's extensive career in Infosec has been dedicated entirely to supporting healthcare environments, and his wealth of experience provides invaluable insights and context from both operational and technological perspectives.

Tamra Durfee

Senior vCISO, Fortified Health Security

Tamra Durfee is an experienced CISO with over 25 years in information security, compliance, regulatory risk, strategy, innovation, and technology transformation. For nearly a decade, she has specialized in healthcare cybersecurity and building risk-based medical device information security programs. Tamra holds certifications as a Certified Healthcare CIO (CHCIO), Certified Digital Healthcare Executive (CDH-E), GIAC Security Leadership Certification, Certified Professional in Healthcare Information Management Systems (CPHIMS), and IBM Certified Solutions Architect.

Jason Stewart

Manager, vCISO Services, Fortified Health Security

Jason Stewart has more than 25 years of progressive experience in the information technology, information security, and cybersecurity industries covering the healthcare, technology, and manufacturing sectors. He excels in complex business management environments with aggressive growth targets and has extensive expertise in advisory services, managed services, strategic governance, threat management, incident response, risk management, education strategies, and board-level advisement.

About Fortified HEALTH SECURITY

Fortified Health Security is healthcare's cybersecurity partner, trusted by healthcare organizations nationwide to deliver tailored, high-touch programs that reduce risk, simplify complexity, and protect what matters most: their patients. As a four-time consecutive Best in KLAS winner, Fortified provides specialized managed security services built exclusively for healthcare.

Fortified understands the full spectrum of healthcare cybersecurity, from rural providers to enterprise networks, third-party vendors, and connected medical devices. The company's award-winning Central Command platform, featuring innovations that translate client feedback into action, enabling smarter, faster security decisions that strengthen every layer of defense.

Fortified doesn't just guard the perimeter. The team embeds with clients, bringing context to every alert and helping healthcare leaders move from reactive to resilient, 24/7, 365.

Because in healthcare, cybersecurity isn't just an IT issue. **It's a patient safety issue.** And Fortified is changing the game.

Learn more at fortifiedhealthsecurity.com.

Fortified
HEALTH SECURITY

www.FortifiedHealthSecurity.com

connect@fortifiedhealthsecurity.com

120 Brentwood Commons Way
Building 4, Suite 500
Brentwood, TN 37027