CitiusTech

Shaping Healthcare Possibilities

CISO's guide to building resilient healthcare

Overcoming cyber threats with confidence

Deepesh Singh
AVP, CitiusTech

Executive Summary

Digital transformation in healthcare is moving forward at a breakneck pace. However, Chief Information Security Officers (CISOs) across healthcare organizations lose sleep over the increasing vulnerability to cyber risks. A whopping 736 healthcare data breaches in 2024 and another 444 reported until August 2025![1] The Change Healthcare Breach of 2024 that impacted 192 million patient records[2] highlights the dangers that healthcare institutions are exposed to. The very systems designed to make care faster and smarter are the ones that hackers now target.

Healthcare's greatest challenge today is this: the same tools that make treatment possible can also make patients vulnerable.

Not going digital is not an option. What if a doctor in the emergency room had to wait hours for an MRI report on a patient to be sent from another branch? That is life-threatening in itself. Every change in technology unintentionally increases the attack surface, exposing mission-critical applications, personally identifiable information (PII), and sensitive protected health information (PHI) to ever-more-advanced cyberthreats.

Using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF 2.0)[3], and insights from actual events, this paper presents strategies that, if implemented correctly, can help heighten resilience and trust in healthcare ecosystems.

The NIST CSF 2.0 Lens: Identify, protect, detect, respond, recover, govern

Building resilience in healthcare isn't about throwing a few security tools into the mix; it's about weaving security into every stage of the lifecycle. We suggest a 6-step approach:

- **Identify:** Keep a live inventory of every user, device, data source, AI agents, API, and flow. This goes beyond just logging them. Organizations need to classify identity based on sensitivity to PHI and PII exposure, centrally visualize & prioritize vulnerabilities, threats, and risks in terms that matter to the business, whether it's HIPAA penalties or reputational fallout.
- **Protect:** Here, the idea is to build a first line of defense with secure identities, data, AI, applications, and APIs with layered controls, such as by enforcing defense in depth, and secure development. The approach is simple: bake security into every stage of lifecycle design, development, deployment, and operations.
- **Detect:** Protection alone isn't enough. Organizations also need to detect potential threats. Ransomware and API abuse don't announce themselves. AI Model breaches and prompt injections are getting bolder. Deploying monitoring SOAR (Security Orchestration, Automation, and Response) mechanisms and solutions to catch anomalies before they spread can be highly effective.
- **Respond:** In the event of an attack, the faster you can move, the smaller the damage. Incident-response playbooks aren't "nice to have"; they're the fire drills for containing malware uploads, API or AI model abuse, or insider threats.
- **Recover:** Of course, incidents will still happen, which is why recovery is critical. Immutable backups, automated failovers, and solid business continuity planning are what keep downtime from becoming a disaster.
- **Govern:** All these steps are tied together with strong governance. Oversight, supply chain risk management, and compliance monitoring aren't box-checking exercises. They're the disciplines that keep everything consistent and audit-ready, whether under HIPAA, GDPR, or local regulations.

CISOs must recognize that true resilience lies not in reacting to threats, but in anticipating and preparing at every stage.

Risk visibility and management

Organizations must be able to classify the risk points in their infrastructure. One can't protect what one doesn't see. The 2021 Scripps Health ransomware attack[4] illustrates what poor visibility can cost: attackers lingered undetected, leading to weeks of downtime and $112 million in losses. Blind spots often persist because third-party vendors don't always share telemetry, leaving gaps in monitoring. Healthcare CISOs must consolidate telemetry across cloud, applications, and medical devices, and contractually require vendors to provide real-time logs under Business Associate Agreements (BAAs).

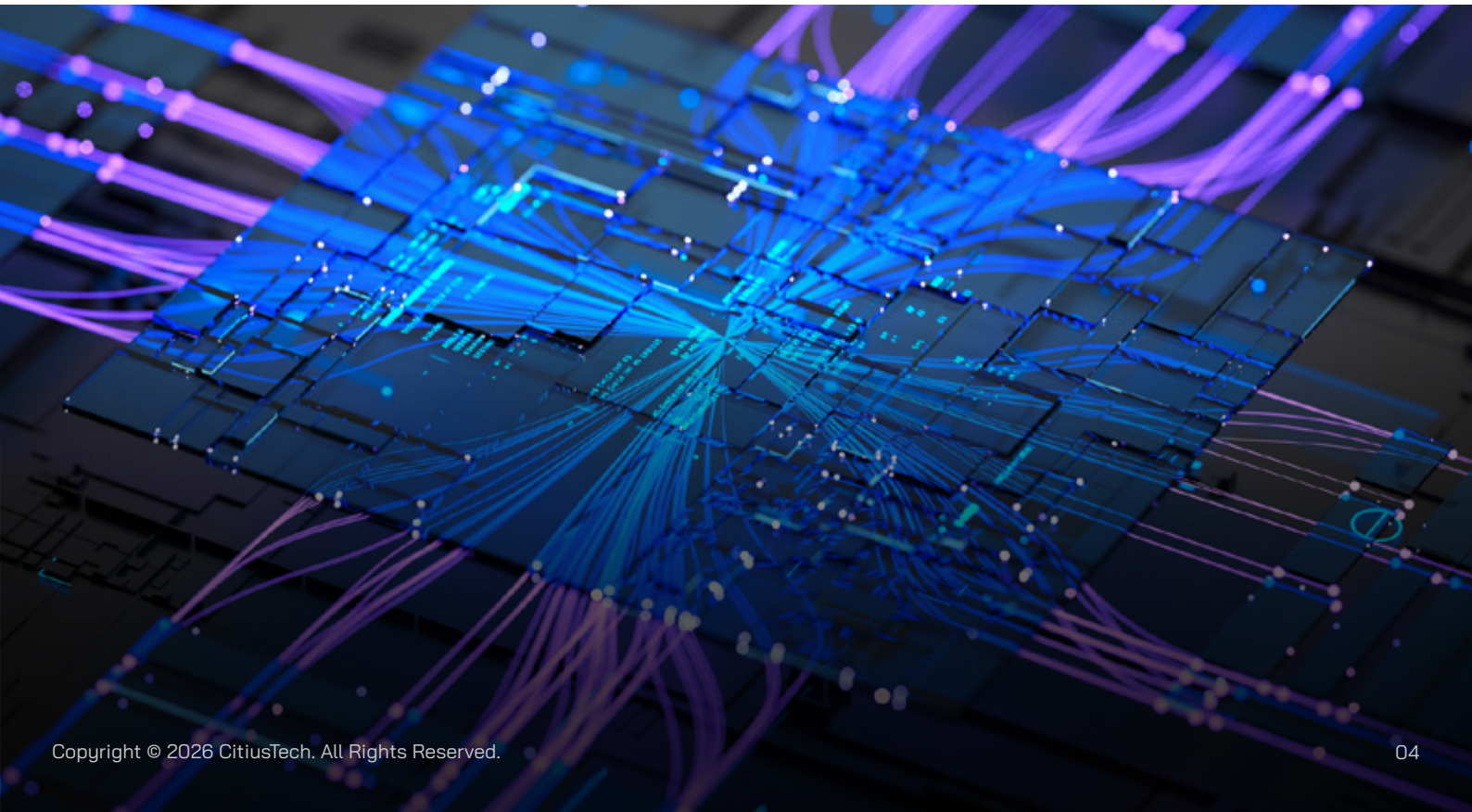
As healthcare increasingly adopts AI for diagnostics, predictive analytics, and operational efficiency, AI systems themselves become high-value targets. The risks listed below pose threats that erode the foundations of AI-powered systems.

- Model poisoning to manipulate training data or inject malicious updates
- Data privacy breaches exposing sensitive patient information
- Adversarial attacks that mislead models and compromise clinical decisions
- Dependency risks from third-party AI services that may introduce compliance gaps

To mitigate these, organizations must implement AI-specific security guardrails for secure design and adoption of AI.

Clearly segregate what is vulnerable (potential exploit), what are the threats (active exploit), and what poses risks (impact). This risk differentiation exercise allows for graded treatments. Healthcare CISOs also need a unified risk dashboard to track vulnerabilities across cloud accounts, biomedical IoT devices, APIs, and human processes.

It also helps to express risk in financial and operational terms, say as cost of downtime, HIPAA/GDPR fines, or patient safety risks.



Identity and access controls

Identity is the real "key to the locker." Digital healthcare ecosystem lockers are opened not just by humans but also by connected devices, APIs, and even AI agents.

The Anthem breach of 2015, which exposed 79 million patient records, stemmed from compromised credentials. An MRI machine or IoT monitor is effectively another user on the network, and without proper identity checks, a rogue device could easily masquerade as trusted equipment. This is why a Zero Trust approach to identity, especially for **Non Human ID's** managed through robust **IGA** frameworks, is essential. Organizations must enforce phishing-resistant MFA (FIDO2/WebAuthn), adopt least-privilege and just-in-time access models, and use AI-driven identity analytics to detect misuse.

Data security governance

Healthcare data flows between EHR systems, analytics engines, insurance platforms, and even outside vendors who print and mail records. Each handoff is a new opportunity for exposure. It becomes an imperative for governance to follow the data wherever it travels.

On the dark web, PHI is worth up to 50 times more than credit card data. The Premera Blue Cross breach of 2015[5] cost 11 million records and a $6.85M HIPAA fine due to weak encryption. From the moment data is classified as sensitive, whether it's PHI, PII, or financial details, it must carry controls (tokenization/masking) that ensure every system touching it maintains the same level of protection.

Beyond encryption and DLP, Data Security Posture Management (DSPM) plays a critical role in healthcare security by providing end-to-end visibility and control over sensitive data. It enables organizations to perform Discovery Classification to identify and classify PHI across structured and unstructured sources, trace data lineage, including Lineage extraction to understand its origin and transformations, and monitor extraction points where data leaves secure environments. DSPM solutions also enforce strict classification and retention policies along with masking and tokenization, while adopting AI to ensure compliance with HIPAA and GDPR. This helps in continuously assessing posture by mapping how data moves through APIs, cloud stores, SaaS platforms, and third-party systems, highlighting misconfigurations and exposure risks. By integrating lifecycle components, including classification, lineage tracking, access governance, and real-time risk scoring, healthcare organizations can proactively manage data security, reduce blind spots, and prevent breaches before they impact patient safety or regulatory compliance.

Governance must extend to model training as well, with proper masking and sanitization to prevent prompt injection[6] or the accidental leakage of personal details.

Securing the application stack

Applications power digital healthcare. These need to be secure by design. Security must be present at every step of the development lifecycle - during design, coding, and repository management, as well as in testing and deployment. The OCR is actively investigating hospitals that embedded tracking pixels (such as Meta Pixel and Google Analytics) on patient portals, which transmitted PHI to third parties, a HIPAA violation. Similarly, insecure CI/CD pipelines and third-party SDKs in patient apps introduce vulnerabilities at scale. Secure SDLC practices, API protection, and AI-driven code scanning must therefore become standard practice.

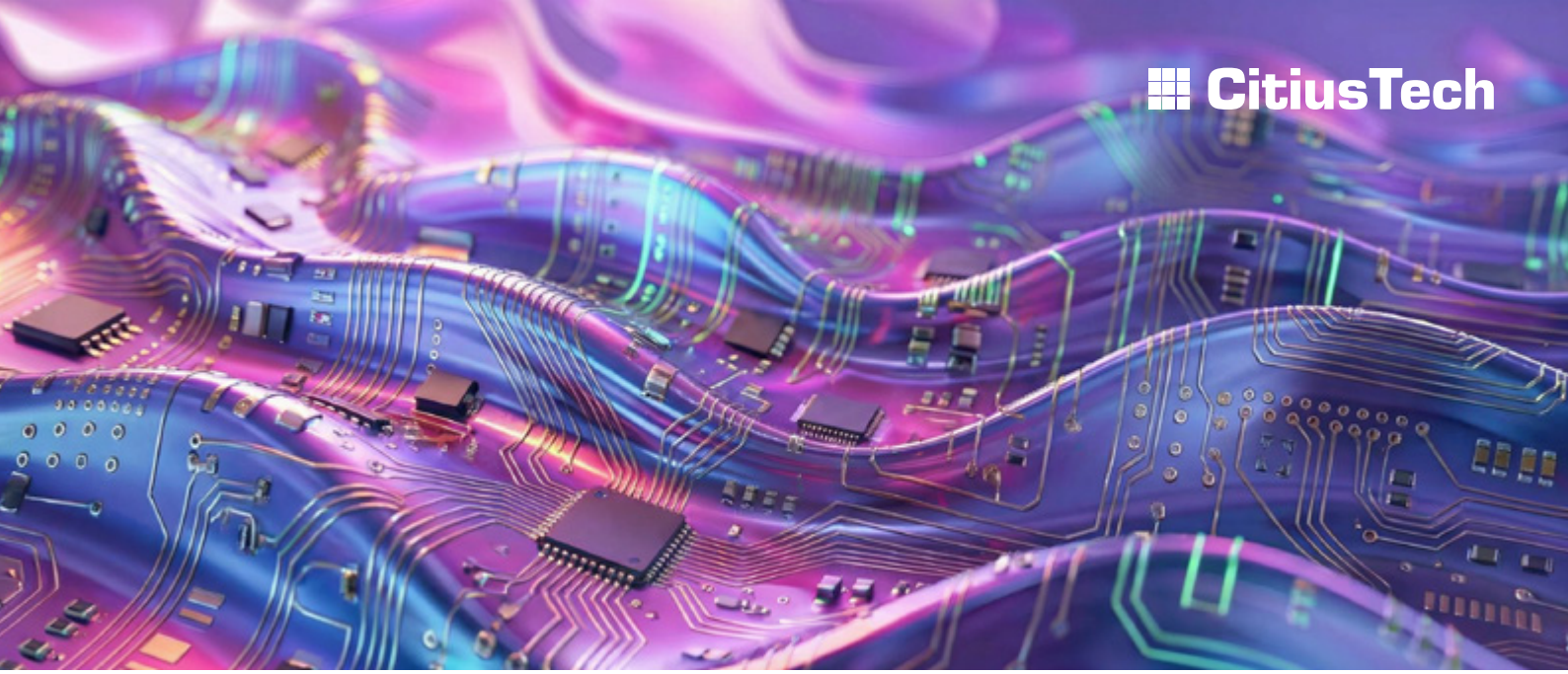
It means keeping secrets out of codebases, ensuring runtime environments are hardened, and applying real-time vulnerability scanning once systems go live. APIs must be protected with firewalls and gateways, and application logic needs regular reviews to spot weaknesses before attackers do.

Threat management and recovery

At no time is your defense 100% secure, as hackers are always trying to discover weak points they can exploit. HHS, CISA, and FBI advisories regularly warn about threat groups like BlackCat and Black Basta, yet many organizations still struggle to operationalize this intelligence. To counter this, organizations need multiple layers of defense that minimize the impact of an attack and strengthen overall **Ransomware Resiliency.** This layered approach also allows businesses to get back on their feet faster, consider immutable backups for recovery. Businesses must also work on alternative paths to maintain operations in the face of a cyberattack. Business continuity plans (BCPs) with immutable backups, ransomware-resilient architectures, and processes must be in place and tested for effectiveness. Red team exercises must reproduce real-world attack possibilities to give security teams a chance to fix loopholes ahead of time.

Platform security and cloud perils

A misconfigured identity, exposed API, or unsecured data pipeline can lead to catastrophic breaches involving PHI and sensitive research data. The attack surface expands with **Multicloud** adoption, biomedical IoT devices, **AI platforms**, and third-party integrations, creating blind spots that attackers exploit. AI introduces additional risks, like models trained on sensitive patient data can be poisoned, inference pipelines can be manipulated, and adversarial inputs can compromise clinical decisions or fraud detection systems. Poor visibility into data flows, model lineage, and API exposure further amplifies these risks, leaving organizations vulnerable to ransomware, compliance violations, and patient safety incidents.



So how do you stay on top of it?

Cloud and SaaS adoption bring agility and scale, while APIs mandated by CMS and ONC (such as FHIR and SMART) are transforming interoperability. However, this progress also creates dependency on third parties and introduces concentration risk.

- Keep running those posture checks. They act like routine health screenings for your cloud instances, APIs, and connected medical devices. If you're not testing and hardening often, you're basically inviting risk.
- Stay on top of your inventory. Know what is in your ecosystem and make a list of blind spots.
- Embrace Zero Trust. Give users only the access they really need, segment when possible, and design with identity as the focus. For instance, platforms like Epic and Cerner have patient data constantly flowing through FHIR APIs, and so they need to be under scrutiny.
- Healthcare organizations must architect for resilience, assume platforms will fail, pre-stage downtime workflows, and demand SOC 2 or HITRUST certification from their vendors.
- To address these challenges, organizations must adopt a layered approach combining Identity Access Management, Attack Surface Management (ASM), Cloud Security Posture Management (CSPM), and Data Security Posture Management (DSPM).

Always on one's toes

AI now plays both sides of the security battle. Leveraging AI effectively can be the difference between catching an intrusion in minutes or weeks. In the healthcare sector, one cyber-attack can put much-needed care for patients in suspension. One successful breach is all it takes to permanently destroy trust. And so, the onus is on the CISOs to be aware of the latest security developments and embed them in their enterprise to make it harder for threats to breach.

References:

1. Healthcare data breach statistics (hipaajournal.com)
2. Nebraska AG's lawsuit against Change Healthcare survives motion to dismiss (hipaajournal.com)
3. Cybersecurity framework (nist.gov)
4. Scripps health ransomware attack cost increases to almost $113 Million (hipaajournal.com)
5. Premera Cross cyberattack exposed millions of customer records (npr.org)
6. Prompt injection attacks on vision language models in oncology (nih.gov)

CitiusTech

Shaping Healthcare Possibilities

www.citiustech.com

About CitiusTech

CitiusTech is a global technology services, consulting, and business solutions enterprise 100% focused on the healthcare and life sciences industry. We enable 140+ enterprises to build a human-first ecosystem that is efficient, effective, and equitable. Leveraging deep domain expertise and next-generation technologies, including AI, Cloud, Data, and Intelligent Automation, we assist our clients to realize their vision, accelerate transformation, and achieve business outcomes. With 7,700+ healthcare technology professionals worldwide, CitiusTech powers digital innovation, business transformation, and industry-wide convergence through next-generation technologies, solutions, and products. Follow CitiusTech on Twitter or LinkedIn.