CitiusTech
Shaping Healthcare Possibilities

PERSPECTIVE PAPER

The high stakes of healthcare cybersecurity in the GenAI era

Vipin Varma
SVP, Head of Cybersecurity Practice, CitiusTech

Abstract

Applications using artificial intelligence (AI) technologies to provide critical care and with access to sensitive PHI are the new reality now more than ever. Therefore, there's a need for a robust and responsive cybersecurity posture in the healthcare sector. Recent incidents prove that healthcare infrastructure is an increasingly attractive target for malicious actors seeking to exploit vulnerabilities and disrupt services, with real-world consequences for patients.

While acknowledging AI's potential to enhance healthcare, organizations need stringent cybersecurity and data governance practices in place to ensure the quality, integrity and confidentiality of sensitive patient data as well as critical systems and applications.

This paper covers the 'security by design' approach, embedding security measures throughout the lifecycle of AI systems. It underscores the importance of securing interconnected systems, including the software supply chain and the burgeoning Internet of Medical Things (IoMT), which pose unique challenges as medical devices become increasingly networked and data-driven.

Content

Introduction

A **majority of healthcare leaders**[1] are either already using GenAI tools or are testing them for mainstream applications often providing or impacting critical patient care. However, this digital transformation, thereby, digital exposure, has created a fertile ground for cyberattacks. With nearly **100 million individuals**[2] falling prey to personal data compromise in 2023 due to cyber incidents targeting healthcare organizations, the substantial financial loss – **60% higher**[3] than the global average – barely scrapes the surface. The bigger picture is a clear depiction of the loss of human value and disruption in patient care and safety, and not just the inconvenience of a lost virtual commodity.

To address this escalating risk, healthcare organizations have refocused their approach to cybersecurity over the past few years. From an afterthought, security has evolved into a strategic imperative, driven by regulatory mandates such as HIPAA and GDPR and patients' increasing demand for breach-proof security measures to safeguard their personal information.

Safeguarding data: Aligning healthcare IoT with information security

More than half[4] of internet-connected healthcare devices designed for on-demand, personalized, value-based care pose a significant risk to personally identifiable information (PII)'s confidentiality and impact on wellbeing due to device functionality. Secondly, the loss of medical data is irreversible. Once compromised, compliance with data privacy regulations becomes extremely complex, especially when dealing with large volumes of historical medical data.

To keep pace, healthcare organizations must focus on building a resilient value chain for hardware and software components to continue strategically reducing risks to an acceptable threshold at the connected device level.

Device Security

Manufacturers of medical devices must embed disruption-ready security measures throughout the device's lifecycle, from design and development to manufacturing and deployment.

Access Controls

Employ role-based access control (RBAC) to limit who can access and modify patient data based on job functions.

Proactive Risk Management

Conduct comprehensive risk assessments to identify potential vulnerabilities and develop mitigation strategies. Stay informed about emerging threats and update security measures accordingly.

AI-powered Threat Analysis

Leverage AI-powered security solutions to detect and respond to cyber threats in real-time. These tools can analyze network traffic, identify anomalies, and detect potential breaches.

Data Encryption

Encrypt data both in transit and at rest to protect it from unauthorized access. Use dynamic encryption algorithms and regularly update encryption keys.

Incident Response Planning

Develop a comprehensive incident response plan to address security breaches effectively. This plan should outline steps to contain the breach, investigate the cause, and recover from the incident.

Data Backups

Regularly back up patient data to ensure that it can be restored in case of a data loss event. Store backups in a secure location and test them periodically to verify their integrity.

Figure 1: Ways to reduce cyber risk for connected devices

GenAI and cybersecurity: Balancing the innovation scales

At the foundation of any successful GenAI implementation is the quality of the data it processes. High-quality, unbiased data is essential to ensure that AI outputs are accurate, equitable, and reliable. Healthcare data, in particular, is diverse, complex, and irreversible (unlike passwords), encompassing medical histories, diagnostic information, treatment records, and genomic data, all of which must be carefully curated to avoid introducing errors or biases into the AI model. Poor data quality can lead to skewed results, reinforce health disparities, or produce outputs that are not clinically actionable.

Adhering to HIPAA compliance and a comprehensive data governance framework based on recommendations developed by NIST, the MITRE Corporation, and the Open Web Application Security Project (OWASP) , apart from others, is, therefore, critical for maintaining data integrity. This includes setting stringent standards for data collection, processing, and maintenance, as well as implementing regular audits to detect biases or inconsistencies in the data. By ensuring that only high-quality, representative data is used to train GenAI models, healthcare organizations can mitigate risks and improve the accuracy of AI-generated insights. In addition, ethical guidelines for data handling, including patient consent and privacy protections, must be rigorously followed to uphold trust in the use of AI within healthcare settings.

Given healthcare data can directly impact life-or-death outcomes, the inherent risks associated with GenAI, like bias, hallucinations (fabricated or inaccurate results), irreproducibility of results, and the opacity of AI decision-making processes (lack of explainability) necessitate operational best practices. This must be underpinned by synergies of cybersecurity, data quality, and ethical usage.

- **Shields up: Designing GenAI systems with security in mind**

  Security should be a cornerstone of GenAI system design, particularly in healthcare, where sensitive patient data is at stake. GenAI systems must be inherently equipped to detect and counteract potential security breaches in real time. To achieve resilience against cyber threats, healthcare organizations must adopt a proactive approach with multiple layers of defense that anticipates and addresses potential risks before they materialize. This can help healthcare organizations shield themselves from data leaks, breaches, and malicious manipulations of GenAI tools. Such a proactive stance is also pivotal in safeguarding the confidentiality and integrity of patient information in this interconnected environment.

- **All checked: Validating outputs of GenAI models**

  One of the critical challenges with GenAI is ensuring that the generated outputs are accurate and clinically relevant. Healthcare organizations must establish validation protocols for GenAI models involving rigorous testing against real-world scenarios and clinical datasets. These validation processes should be continuous and iterative, allowing healthcare professionals to regularly assess the model's performance and accuracy. Cross-disciplinary collaboration between data scientists, clinicians, and ethicists can also enhance the validation process, ensuring that AI outputs align with medical best practices and ethical standards.

- **Alert: Securing endpoints and data from GenAI-powered medical devices and wearables**

  Connected medical devices and wearables generate sensitive patient data that requires robust security. Protecting both the data collection points and the aggregation locations is essential. Continuous measurement and monitoring of cybersecurity protocols are necessary as the IoMT expands, creating new cybersecurity challenges.

- **Knives out: Protecting against prompt injection and adversarial attacks**

  GenAI systems, particularly those that interact with user inputs (prompts), are vulnerable to manipulation through prompt injection and adversarial attacks. These types of attacks can distort the model's outputs or compromise the integrity of sensitive healthcare information. To counteract this, healthcare organizations must implement robust access controls, data encryption, and secure AI model management. The specialized defenses include sanitizing input prompts, incorporating anomaly detection algorithms, and developing AI models that can identify and resist adversarial manipulations. Adhering to the principle of least privilege, constant monitoring of system behavior and outputs is essential to detect and mitigate potential threats before they can cause harm.

- **Eyes on target: Avoiding "excessive agency" and ensuring human oversight**

  While GenAI can provide valuable insights and decision-support tools in healthcare, it is crucial to avoid over-reliance on AI-generated outputs. Human oversight remains a critical factor in ensuring responsible and effective usage of AI tools. Healthcare providers must maintain a "human-in-the-loop" approach, where clinicians validate and interpret GenAI outputs before making critical decisions. This ensures that AI tools augment, rather than replace, human expertise, preserving the clinician's authority and judgment in patient care. Additionally, stringent monitoring and assessment of GenAI systems should be implemented to identify potential failures or inaccuracies, further reinforcing trust and accountability in AI usage.

Fortifying healthcare cybersecurity: Leading from the front

As healthcare continues its digital transformation, the urgency for strengthened cybersecurity measures cannot be overstated. The growing complexity of healthcare technology demands ongoing investment in robust cybersecurity infrastructure, encompassing not only advanced tools and technologies but also the training and development of skilled professionals.

AI is not a black box; healthcare leaders must understand both its capabilities and risks. AI offers a promising frontier for enhancing cybersecurity, with its capacity to detect and mitigate threats in real-time. Organizations must be proactive against emerging cyber threats with an approach that includes regular updates, security protocols, and ongoing collaboration with industry experts. While there is a race to adopt cybersecurity measures amidst the GenAI era and IoMT ecosystem, the challenge lies in its effective implementation. Given the universal aspiration for protection, all parties seek to establish robust defenses. Healthcare leaders must invest in skilled professionals, robust cybersecurity infrastructure, and partnerships with industry experts to navigate the evolving landscape of cyber threats.

CitiusTech plays a pivotal role in this effort, offering a range of services, including governance, risk, and compliance (GRC), attack surface management, cyber defense operations, data protection, identity and access management (IAM), and cloud security. Our security solutions for healthcare platforms, medical technology, and medical devices equip organizations with the tools and knowledge to drive innovation in patient care.

References

1. Generative AI in healthcare: Adoption trends and what's next (mckinsey.com)
2. Healthcare cyberattacks have affected more than 100 million people in 2023 (chiefhealthcareexecutive.com)
3. What is the cost of a data breach? (forbes.com)
4. Healthcare cybersecurity: A global imperative (forbes.com)

CitiusTech

Shaping Healthcare Possibilities

CitiusTech is a global IT 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 with deep domain expertise and next-gen technology.

With over 8,500 healthcare technology professionals worldwide, CitiusTech powers healthcare digital innovation, business transformation and industry-wide convergence through next-generation technologies, solutions, and products.

www.citiustech.com

Shaping Healthcare Possibilities