VIEW POINT

EMERGING GAPS IN HEALTHCARE SECURITY

Abstract

Convenience, more accessible healthcare, and better patient care are some of the major benefits of the healthcare industry embracing digital transformation with electronic patient records, interconnected databases, and telehealth and mobile health applications. However, this has the downside of making healthcare data the number one target for cyberattacks. Healthcare service providers' lack of understanding of data security risks, lacking security protocols in telehealth and mobile health applications, outdated medical systems and lacking cybersecurity policies and protocols have made healthcare systems a soft target for cyber attacks, impacting millions of people every year. But with proper training, regular security audits and integration of stringent cyber resilience protocols, the healthcare industry can address the emerging gaps in healthcare security and protect patients' sensitive data from cyberattacks.

Infosys®
Navigate your next

Cyberattack is common risk businesses have to account for in their journey toward digital transformation. However, where many industries take the cybersecurity risk seriously and attempt to keep evolving with the emerging threats and cyber attacks, the healthcare industry finds itself increasingly vulnerable to cybersecurity threats as the years pass. Between 2020 and 2022, there was a 69% increase in healthcare security breaches, which impacted 45 million people in 2021 alone (up from 34 million in 2020). These attacks not only hamper the healthcare providers' ability to service the patients but costs millions of dollars for healthcare providers to remediate, with an average ransomware attack costing USD 1.27 million and an average data breach costing USD 9.23 million. Despite the healthcare industry investing USD 125 billion in cybersecurity, healthcare data remains vulnerable to the perpetual threats of cyberattacks and data breaches.

Healthcare systems: An attractive target for cyber attacks

Are healthcare systems an attractive target for cybercriminals? The answer is a resounding yes. A shared healthcare system makes patients' lives safer while at the same time exposing them to risk. While more data makes providing quality healthcare easy, this data can be a magnet for criminals. Medical data not only gives access to the private information of thousands of patients but also opens doors to the confidential financial information of medical service providers.

Cybercriminals often gather data to sell for ransom or exploit it for personal use. Attackers can use the insurance information to undergo expensive medical treatments for themselves or get prescription medication under a patient's name. They could also directly attack a healthcare organisation by encrypting files or locking services and holding the data for ransom. As healthcare is a time-bound service and a matter of life and death, healthcare providers often have no choice but to pay the ransom to the attackers.

It is, hence, imperative to continually monitor security breaches in the healthcare industry and address them as per legal guidelines like the Health Insurance Portability and Accountability Act (HIPAA) or the General Data Protection Regulation (GDPR). Not only is there an ethical commitment to patients worldwide to safeguard their personal information, but it is also true that healthcare security breaches could damage people's lives.

Biggest data security challenges for the healthcare industry

In addition to being an attractive target for cybercriminals, healthcare systems have been the number one soft target for cyberattacks for over a dozen years. And despite increasing investment in healthcare security, data security concerns continue to bother the healthcare industry, continually making it an easy target. Some of the biggest data security challenges facing the modern healthcare industry include the following:

• **Growing attack surfaces:** The healthcare industry is moving away from paper records and towards Electronic Health Records (EHRs) for timely and efficient patient care. However, this has also increased the number of attack surfaces available that leave many healthcare providers vulnerable. As a result, ransomware attacks have become prevalent in the healthcare industry.

• **Healthcare data vulnerabilities:** The sensitive nature of healthcare data makes it highly vulnerable to cyberattacks. Hackers can use information like medical history, personal details, and insurance information of patients and financial (or billing) information of patients and healthcare service providers for many nefarious purposes. Easy access to centralised patient databases through EHRs makes it easier for cyber criminals to steal patient information and profit from exploiting it.

• **Telehealth services and mobile medical applications:** Digital transformation in the healthcare industry has shifted towards offering telehealth services or mobile medical applications to make healthcare services more accessible. These applications may lack stringent data security protocols. Additionally, these services also give patients more control over their medical data, and individuals may share their credentials or be lax in adopting security protocols, such as multi-factor authentication or complex passwords. This can lead to data breaches and leave healthcare data vulnerable.

• **Internet of things (IoT) security vulnerabilities:** IoT has augmented many healthcare services, making them more efficient and accessible; it has also increased the security risk as IoT devices are prone and vulnerable to cyberattacks. Although the increased connectivity is something to be hopeful about, IoT devices need to implement better security protocols to protect sensitive medical information.

• **Outdated medical hardware and software:** With limited resources, healthcare service providers are still using medical devices and IT systems that are decades old, with software the manufacturers no longer support. Additionally, even the newer devices have lax security control, leaving a virtual jackpot of patient data up for grabs for anyone with an understanding of their vulnerabilities and the intention of exploiting them.

• **Healthcare systems are interconnected:** With attempts at digital transformation and increasing connectivity, all healthcare service providers and insurance companies now have access to a centralised patient database, which fetches data from EHRs. Although this connectivity increases convenience and coordination between different service providers, it also increases vulnerabilities to cyberattacks, as vulnerability with even one service provider can compromise the entire database.

• **Smaller providers struggling to keep up:** As gaps in healthcare data security are becoming clearer, bigger hospitals are actively investing in IT infrastructure for better security. Smaller healthcare service providers, however, struggle to keep up with the pace of digital transformation along with planning for cybersecurity measures. As a result, cyber attackers target smaller hospitals and clinics to gain access to interconnected patient databases through their systems.

• **Lack of cyber security education and awareness:** Insider threats are ever present when discussing healthcare data security. These threats are not always necessarily malicious but can stem from a lack of awareness and ignorance as well. Many healthcare service providers are unaware of data security risks and the role they must play in securing patient data. As a result, nearly a third of data breaches result from accidental data leaks from unaware employees. This lack of awareness can also lead to ransomware attacks or healthcare service providers falling victim to phishing attacks.

• **Healthcare service providers often ignore cybersecurity risks:** Lack of training, understanding, or awareness about data security risks leads to healthcare providers often ignoring cybersecurity risks with a mindset of "it will never happen to me". As a result, hospital administrators often direct the limited resources away from cybersecurity protocols, leading to a lack of encryption for protecting sensitive data and weak protections for websites, servers, and databases. This gives cybercriminals an easy in into healthcare data.

• **Lacking cybersecurity policies and procedures:** As a result of ignoring cyber security risks, healthcare service providers often have no personnel dedicated to securing their data. This lack of clear structure, security policies, procedures, and protocols increases the risk to healthcare data security.

Best practices to address healthcare security issues

The healthcare industry has a responsibility towards the people it serves to safeguard the personal and medical information of the patients. Employee training and awareness, stringent security protocols, regular audits, and cybersecurity expert intervention can help curb data loss. Some of the best practices to address healthcare data security issues include:

- Ensure legal compliance at every stage.
- Increase investment in cybersecurity for integrated security solutions, modern infrastructure, and improved visibility across systems.
- Implement advanced data encryption for all healthcare data at every stage (storage and transit).
- Require multi-factor authentication for telehealth and other mobile medical applications.
- Allow selective data access.
- Maintain secure data backups at offsite locations.
- Conduct regular risk assessments and audits.
- Deploy robust logging procedures to track who is accessing patient data, when, and why.
- Use solutions like virtual private networks (VPNs) or mobile device management (MDM) when remote.
- Raise awareness about cybersecurity risks among healthcare service providers and train them to identify threats to healthcare data security.
- Build cyber resilience with a zero-trust security and threat-centric approach.
- Leverage automation, artificial intelligence, and machine learning solutions to detect and prevent cyberattacks.

Raising awareness about cybersecurity risks and embracing these practices can be the first step in addressing the healthcare security gaps and securing the personal and medical information of patients.

Conclusion

As the healthcare industry is embracing digital transformation – with electronic health records, telehealth mobile applications, and interconnected databases for more cohesive care – several gaps in healthcare security are also emerging, which leave healthcare data vulnerable to attacks. Growing attack surfaces, outdated medical systems, lack of cybersecurity awareness among healthcare service providers, and virtually non-existent data security policies and protocols are some of the biggest data security challenges facing the modern healthcare industry. Modernising healthcare infrastructure, raising cybersecurity awareness, and leveraging automation solutions to build cyber resilience are necessary if the healthcare industry wants to protect sensitive patient information while embracing digital transformation for more convenience and better patient care.

* For organizations on the digital transformation journey, agility is key in responding to a rapidly changing technology and business landscape. Now more than ever, it is crucial to deliver and exceed on organizational expectations with a robust digital mindset backed by innovation. Enabling businesses to sense, learn, respond, and evolve like a living organism, will be imperative for business excellence going forward. A comprehensive, yet modular suite of services is doing exactly that. Equipping **organizations with intuitive decision**-making automatically at scale, actionable insights based on real-time solutions, anytime/anywhere experience, and in-depth data visibility across functions leading to hyper-productivity, Live Enterprise is building connected organizations that are innovating collaboratively for the future.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next