HealthManagement
Promoting Management and Leadership

Protecting Telemedicine from Cyberattacks: Strategies for Healthcare Leaders

The rise of telemedicine has profoundly transformed healthcare, offering unprecedented convenience and accessibility to patients. However, its rapid expansion has also created a lucrative target for cybercriminals. With sensitive patient data and critical healthcare operations at stake, the security of telehealth systems is an urgent priority. By adopting proactive measures, healthcare organisations can ensure data protection, maintain patient trust and comply with industry standards.

Telehealth's Expanding Attack Surface

Telemedicine platforms present numerous vulnerabilities that cybercriminals can exploit. Commonly employed tactics include phishing scams, malware and ransomware attacks. Phishing, for instance, tricks users into revealing login credentials or downloading malicious software, allowing attackers to infiltrate systems. Once inside, cybercriminals can steal, encrypt or corrupt sensitive data, often neutralising backups to exacerbate the damage. The complexity of telehealth operations further amplifies these risks.

Outsourced telehealth providers are particularly vulnerable due to their extensive integration with multiple health systems. A single breach at a third-party provider could expose a vast network of interconnected organisations. Additionally, many telehealth providers rely on personal devices and home networks for their work. These environments often lack robust security measures, such as properly configured routers or controlled access, making them susceptible to intrusion. This "Bring Your Own Device" (BYOD) culture, compounded by inadequate home network security, creates significant cyberattack exposure.

Beyond the risks associated with infrastructure, the access requirements of telehealth providers elevate their value as targets. Virtual providers often have privileged access to electronic health records (EHRs), prescribing systems and financial platforms, including patient payment information. This multifaceted access consolidates a wealth of sensitive information, making telemedicine delivery a high-value target for cybercriminals.

Strengthening Cybersecurity Measures

To address these vulnerabilities, healthcare Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) must prioritise robust, multi-layered security strategies. Conducting comprehensive risk assessments of outsourced telehealth providers is a critical first step. These evaluations should examine technical, administrative and physical controls, ensuring that virtual providers adhere to strict protocols for identity proofing, credentialing and ongoing monitoring. This includes implementing level-of-assurance controls for activities such as prescribing controlled substances, where stricter verification processes are required.

Securing network infrastructure is equally essential. Telehealth providers should operate in controlled environments or employ secure, encrypted connections, such as Virtual Private Networks (VPNs). However, VPNs alone are not infallible, and additional safeguards, such as endpoint security and firewalls, are necessary to enhance protection. Healthcare organisations should also establish isolated network access points within their IT infrastructure. This ensures that breaches originating from telehealth providers do not compromise core systems or sensitive patient data.

Another strategy is monitoring compliance with security practices. Regular phishing simulations and penetration tests help identify vulnerabilities, while ongoing credential reviews prevent unauthorised access. Moreover, operational agreements with telehealth providers should clearly define responsibilities for securing sensitive functions, such as processing payments and safeguarding prescription data. Organisations must ensure continuous monitoring and evaluation of their telehealth providers' security measures and be able to adjust protocols as threats evolve.

A Proactive Approach to Cybersecurity

To achieve comprehensive protection, healthcare organisations must integrate telehealth security measures into their broader cybersecurity framework. This holistic approach views telehealth providers as extensions of the health system, necessitating the same level of scrutiny and risk management applied to internal operations. Such integration allows organisations to track telehealth providers' progress in mitigating risks and ensure alignment with security objectives.

Compliance with industry standards is a critical component of this strategy. The Health Insurance Portability and Accountability Act (HIPAA) provides baseline security requirements for managing risks and responding to breaches. However, frameworks like HITRUST go beyond HIPAA, offering a more comprehensive approach by incorporating international standards. Adopting these advanced frameworks can strengthen defences and simplify compliance across multiple jurisdictions.

Regulatory developments are also shaping the cybersecurity landscape. States such as New York have introduced requirements that exceed HIPAA standards, reflecting a growing recognition of telehealth's unique challenges. At the federal level, proposals from the White House and Congress aim to enhance accountability and encourage stricter cybersecurity practices. These initiatives signal a broader push toward standardisation, ensuring that healthcare organisations adopt measures to safeguard patient safety and data integrity.

Telemedicine has become integral to modern healthcare delivery, but its convenience comes with substantial cybersecurity risks. By understanding the vulnerabilities inherent in telehealth systems and implementing targeted multi-layered defences, healthcare organisations can protect sensitive patient data and maintain the trust of those they serve. Integrating telehealth security into a unified cybersecurity strategy and staying ahead of regulatory requirements will ensure that telemedicine remains a secure and reliable option for the future of healthcare delivery.

Source: **Healthcare IT News**

Image Credit: **iStock**

Published on : Tue, 26 Nov 2024