Alberta Doctors' Digest

Don’t get hacked!

In a significant data breach, hackers infiltrated the IT systems of five major hospitals in southeastern Ontario, including Windsor Regional Hospital. This cyberattack occurred in October 2023 and has had profound repercussions. Windsor Regional Hospital lost access to its electronic health records and email services for months. Experts estimate that the hospital will require most of 2024 to fully recover.

This breach underscores a troubling trend of escalating cyberattacks and highlights the growing frequency and severity of such breaches in the health care sector. Owing to its vast reservoirs of sensitive data, the health care sector has become a primary target for cyberattacks. Physicians, tasked with the crucial responsibility of patient care, are increasingly vulnerable to cyber threats. Those who manage their own medical practices bear the dual duty of upholding patient data confidentiality and safeguarding the integrity of medical systems.

Cybersecurity risks

Physicians managing their own practices face several significant cybersecurity risks.

Patient data breaches: Medical practices store vast amounts of sensitive patient information, making them prime targets for cybercriminals aiming to exploit this data for identity theft or financial fraud. Such breaches can result in severe legal and economic repercussions for the practice.

Ransomware attacks: Medical practices are vulnerable to ransomware attacks that encrypt files and block system access, often demanding ransom payments to restore critical patient data.

Phishing attacks: Medical practitioners and their staff are frequently targeted through phishing emails. These can be disguised as urgent patient requests or official communications from health care organizations. These emails threaten sensitive information when recipients are deceived into revealing it or clicking on malicious links.

Inadequate infrastructure and security practices: Small medical practices often need more resources or expertise to implement robust cybersecurity measures, leaving them vulnerable to cyber threats. Outdated software, weak passwords, unpatched systems, and inadequate employee training all contribute to potential vulnerabilities cybercriminals exploit.

Cybersecurity recommendations

To help clinics and hospitals prevent, mitigate and navigate cyberattacks, the US National Institute of Standards and Technology has the following recommendations.

Prevention: Experts emphasize the importance of implementing robust preventive measures to safeguard health care data. These include installing anti-virus and VPN

software across all devices, adopting strong password policies coupled with two-factor authentication, and maintaining up-to-date software.

Detection: It is crucial to recognize the signs of a potential cyberattack. Warning indicators may include anomalous activities such as unexpected pop-up messages, emails from unfamiliar sources, or the presence of unrecognized files. Anti-virus and malware scans can help identify and mitigate these threats promptly.

Response: In the event of a cyberattack, swift action is paramount. The initial steps involve disconnecting affected machines from the internet and powering them down. The Canadian Medical Protective Association (CMPA) advises notifying patients immediately in the event of a suspected breach, with law enforcement involvement recommended, particularly in cases of ransomware attacks.

Recovery: The ability to swiftly recover from a cybersecurity incident hinges on robust data recovery mechanisms and external backup within health information systems.

Training: Regular training sessions should educate employees on best practices, including identifying phishing attempts, securing personal devices, and adhering to stringent password protocols.

While no approach can guarantee absolute immunity, combining technological defences, stringent policies, and ongoing training significantly decreases the risk of becoming another victim of cyberattacks.

Reference: *Cyberattacks on Canadian health information systems. CMAJ, 195(45), E1548-E1554. Harish, V., Ackery, A., Grant, K., Jamieson, T., & Mehta, S. (2023).*

Banner image credit: pixabay.com