How Healthcare Providers Can Prepare for Privacy Breaches

October 7, 2020

According to studies by PWC and the SANS Institute, 94% of healthcare organizations have been victims of a cyber attack. (1)

In the COVID-19 era, healthcare organizations have been hit harder than ever. In August, Nova Scotia Health was the victim of a data breach in which 211 patients had their personal health information inappropriately accessed.

Karen Hornberger, the provincial director of privacy found that two employees from two separate hospitals in New Glasgow and Kentville had inappropriately accessed the hospital's scheduling system and medical records system over the course of two years. (2)

Major healthcare organizations take privacy seriously. Unfortunately, no one is immune to the threat of cybercrime. As Hornberger stated, “the health authority’s proactive auditing program aims to stop these incidents from happening, however it isn’t always successful.” (2)

Dangers of a Privacy Breach

Privacy breaches can occur on any technological device where data is stored. This includes on wearables, such as fitness trackers, implantables, such as insulin pumps, and hospital equipment, such as x-ray machines. Following are some of the key vulnerabilities:

- **Patient data theft:** Thieves don’t just crack computers and hospital equipment. They can also extract the sensitive user data in software found on wearables, such as fitness trackers.
- **Reputation damage:** Studies by PWC and the SANS Institute found that 38% of patients say they would be wary of using a device that had been previously hacked. (1)
- **Therapy manipulation:** As an experiment in data security, one security researcher figured out how to hack his own insulin pump. In doing so, he proved that a deadly overdose of medication could be administered remotely via a vulnerability in certain insulin pumps. (1)
- **Malware:** One infected device can spread, infecting the entire network.

Steps to Prepare for a Privacy Breach

As patient care becomes more digitized, rapid technological innovations have outpaced the legislation needed to protect patient and organizational privacy and security.

Healthcare practitioners need to be sufficiently agile to stay on top of existing policy and regulations, but they also need to go beyond the minimum security requirements to prevent and manage security threats.

The benefits of prioritizing privacy:

- Privacy measures can help preserve a level of trust between the organization and its patients, by either stopping, avoiding, or minimizing reputational damage.
- Privacy measures can help companies in the healthcare field to safely drive business value from sensitive health data.
- Privacy compliance gets healthcare providers ahead of a potential crisis, either reducing the damage of a potential data breach or preventing it altogether.

Tips for healthcare organizations:

1. **Educate staff.** The human element where error and negligence can occur is perhaps the single greatest threat to cyber security in healthcare. Healthcare staff should be equipped with cyber security awareness training so they can make informed decisions and use appropriate caution when handling sensitive patient data.
2. **Restrict access to data and applications.** Another security measure involves restricting access to medical data and applications to only those users who need them to perform their jobs. Many companies use multi-factor authentication (such as a password plus biometrics) for this approach.
3. **Implement data usage controls.** This method helps to flag and block malicious activity in real time. For example, data controls can block specific actions involving sensitive data, such as web uploads, unauthorized email sends, copying to external drives, or printing.
4. **Log, monitor, and assess.** While auditing helps track usage and identify how problems happened, conducting regular risk assessments helps stop potential data breaches before they start.
5. **Get the right insurance coverage.** Knowing the risks and staying vigilant is key, and a consult with a cyber-savvy broker can offer that much more value to healthcare clients looking to protect their data privacy.

Tips for healthcare workers:

1. **Harden passwords.** Though obvious, the measure of creating a strong password is still a highly effective protective measure against hackers.
2. **Secure social media accounts.** Social media channels contain a wealth of sensitive personal data. That is why many social media channels allow users to enable a two-step verification on their accounts. Beyond just a strong password, users can add an additional step where logging in requires entering a security key sent to the user's phone.
3. **Ignore and/or report suspicious links.** Cyber criminals still use fake emails and convincing websites to trick users into a phishing attack. It's always advisable to hover over linked text or images before clicking on them, to see if the URL looks legitimate.

The MedThree Advantage

Cyber insurance can't stop a potential data breach from occurring, but it can help keep healthcare providers and organizations on stable financial ground if a cyber attack occurs. MedThree Insurance Group specializes in writing healthcare risks, while keeping abreast of the nuances and forever changing regulations and guidelines within the healthcare industry. Visit our website for more details.

Content is current as of the date of broadcast and is subject to change without notice.

Sources:

1. https://medicalfuturist.com/five-tips-defending-online-privacy-healthcare-infographic/
2. https://www.canhealth.com/2020/08/05/two-employees-breach-info-of-211-patients-in-ns/