

HOW TO LOWER CYBERSECURITY RISKS IN HEALTHCARE





Healthcare is a prime target for cybercriminals. Protected health information and electronic medical records are a data treasure trove. The threat is real ... and growing. This ebook outlines the cybersecurity risks in healthcare. We also share best practices and benefits of a managed services provider's help.





No wonder adoption could reach 75 billion IoMT devices worldwide by 2025.

The problem is in securing these devices along with existing systems and networks. Healthcare providers store sensitive medical and financial information, and hackers are always developing more ways to gain access to data or hold data and networks for ransom.


The Risks for Healthcare Providers

Let's start with December 2020 examples. GE Healthcare identified two critical vulnerabilities impacting more than 100 of its products. The software vulnerabilities affecting MRI, X-Ray and ultrasound devices allow remote code execution. That allows access or alteration of sensitive patient data.

Also in December:

- Cybersecurity Infrastructure and Security Agency warned of phishing targeting those distributing COVID-19 vaccines.



- 
- A BishopFox Labs researcher identified four vulnerabilities in OpenClinic health record management software.

These three examples help to show the range of issues healthcare providers face. Then, there's the risk of ransomware, which continues to plague the healthcare sector.

One recent example of a ransomware attack affecting the medical industry occurred in November 2020 when the healthcare provider Universal Health Services (UHS) was hit by a ransomware attack that impacted its 250 hospitals and outpatient facilities in the United States. The attack disrupted patient care and forced UHS to divert ambulances and transfer some patients to other healthcare providers.

The ransomware used in the attack was reportedly the Ryuk ransomware, which is known for its ability to quickly spread throughout a network and encrypt files, making them inaccessible to the victim organization. The attackers demanded a ransom payment of \$1.5 million in Bitcoin in exchange for a decryption key to unlock the encrypted files.




While UHS did not disclose whether it paid the ransom, the attack is estimated to have cost the company tens of millions of dollars in lost revenue and recovery costs. In addition to the direct financial impact, the attack also had a significant impact on patient care. The company's electronic health record system was disrupted, forcing healthcare providers to rely on paper records and delaying patient care.

The impact of the attack was felt not only by UHS but also by patients who were affected by the disruption in care. The attack highlights the significant risk that ransomware poses to the healthcare industry, which is increasingly reliant on electronic health records and other digital technologies. When these systems are disrupted or encrypted, patient care can be delayed or even halted altogether.

In addition to the direct financial impact of ransomware attacks on healthcare providers, there are also indirect costs associated with these attacks. For example, patients may choose to seek care elsewhere if they perceive that a healthcare provider's systems are not secure, which can result in a loss of revenue for the provider. In addition, patients may be reluctant to share sensitive health





information if they do not trust that their information is being protected.

The cost of a ransomware attack can vary widely depending on the size and complexity of the healthcare provider's network, as well as the extent of the attack. However, the cost can easily run into the millions of dollars when lost revenue, recovery costs, and reputational damage are factored in. In addition to the financial impact, these attacks can also have a significant impact on patient care, which can have long-lasting effects on patient outcomes.

In conclusion, ransomware attacks pose a significant threat to the healthcare industry, with the potential to disrupt patient care and cause significant financial losses.

Healthcare providers must take proactive steps to protect their networks and patient data from these attacks, including regular training for employees, implementing strong cybersecurity measures, and ensuring that backups of critical data are regularly tested and updated. By taking these steps, healthcare providers can help to minimize the risk of a ransomware attack and protect patient care.



5 Healthcare Cybersecurity Best Practices

#1 Educate healthcare staff


Your employees typically don't mean to endanger data or risk cybersecurity compliance, but cybercriminals are deft at social engineering. They take advantage of current events, and they leverage the human desire to help. Training all new employees thoroughly before they handle any patient data is critical. Create and document a training program, and equip people to make smart decisions and use appropriate caution.

#2 Limit access

Limiting user access to a needs-only basis can help cut damage in the event of human error or a breach. Install access restrictions that require multi-factor authentication.

Ensure authorized users can access necessary patient information and certain applications only.

This includes access controls for:

- 
- all network/server equipment and systems to prevent access and disclosure of patient data;
 - software applications that contain patient data.

Create access and activity logs, and routinely review the logs for suspicious events and respond appropriately. Also, stop user accounts when necessary and appropriate.

#3 Encrypt data

Data encryption is essential at rest and in transit. This makes it difficult to decipher patient information if attackers gain access.

#4 Keep an accurate, thorough technology inventory

Analyse security risks and vulnerabilities. Inventory all systems, programs, and applications that store, send, or receive patient data. This requires securing mobile devices and all those IoMT devices, too.

Securing internet-connected devices requires tactics such as:



- managing all devices, settings, and configurations;
- enforcing the use of strong passwords;
- enabling the ability to remotely wipe and lock lost or stolen devices.

#4 Monitor partners, too

Healthcare information gets transmitted between providers and partners to facilitate payments and deliver care. Regular review of vendor and third-party service provider credentials should be ongoing.

#5 Conduct risk analysis

Assess risk and develop a risk management plan to address any identified vulnerabilities.

A managed service provider (MSP) can help with healthcare security and maintaining compliance.



How a Managed Service Provider Helps

A partnership with an MSP can help healthcare providers shore up their cybersecurity. These IT experts can ensure the best practices enumerated above. Your MSP also takes proactive measures to help prevent future attacks.

The MSP allows doctors, dentists, therapists, orthopaedists, and more to focus on keeping people healthy. Meanwhile, the MSP manages and monitors the IT for vulnerabilities. While keeping up with the latest threats to the industry, an MSP can also make a difference on a day-to-day basis. They recommend technology that helps healthcare providers work more efficiently, and they suggest secure solutions to streamline workflow, enable collaboration, and provide portable access.

Finally, an MSP can bolster data backup procedures and help establish continuity plans. That way, if the worst should happen, the healthcare provider can get you back up and running quickly.

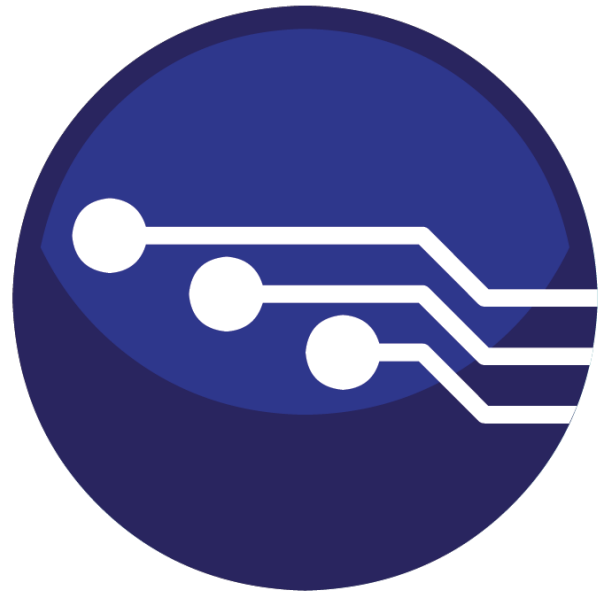


NextGEN IT Solutions has been providing quality IT solutions and support to medical professionals and businesses for over 22 years. They specialize in providing secure and reliable network solutions, cloud solutions, and support for a wide range of medical software applications.

Their team of experts has a deep understanding of the unique needs of the healthcare industry, and they offer a comprehensive suite of IT services to help healthcare providers stay secure, compliant, and efficient. They are committed to providing exceptional customer service..

NextGEN IT Solutions has a proven track record of success in the industry and has helped healthcare providers and businesses stay connected and secure.

Give us a call to discuss your needs and let us be Your IT Partner.



NextGEN IT Solutions

Phone: **(724) 204-1950**

Email: info@nextgen-itsolutions.com

Web: www.nextgen-itsolutions.com