CYBER READINESS
INSTITUTE

Cybersecurity Best Practices for Telehealth

The healthcare landscape looks different now than it did eight months ago. Telehealth is more prevalent than ever before and there are new policies to understand and implement in your practice. Despite all these changes, one issue remains the same: there is an extraordinary amount of personally identifiable, sensitive, and confidential information embedded in our healthcare system.

Questions of access and security have always been important, particularly when practices started to transition to electronic health records. With telehealth growing in popularity, it is now more important than ever to ensure that your medical practice understands and implements basic cyber hygiene behaviors to protect patient and business data. Creating a culture of cyber readiness within your practice will not only reduce your risk of being hacked, but it will also better prepare and equip you with the right tools if and when you are breached. By focusing on human behavior and identifying a point-person, or "Cyber Leader," within your practice, the Cyber Readiness Institute encourages you to focus on education and awareness as your best defense and opportunity for resilience.

Hackers take advantage of gaps in telehealth security to wage targeted attacks on vulnerable medical practices. Researchers found that from March to April of this year, security alerts sent to information technology departments at 148 hosts of the most popular telehealth applications jumped 30% overall as compared to the same period a year earlier.

As the popularity of telehealth expanded, there was a corresponding increase in targeted attacks, including a 117% jump in security alerts just caused by malware infections.

When it comes to matters of telehealth, having a strong foundation in the basics – passwords, software updates, phishing, and USB use – will be immeasurably beneficial as your practice adapts to the new "telehealth environment."

Best Practices

Familiarize yourself with telehealth because it is here to stay

- Acknowledge that the convenience of telehealth makes it attractive to patients
- Understand how declared public health emergencies change your telehealth protocols (i.e. reimbursement, interstate licensure, HIPAA regulations)

Be proactive, not reactive

- Create an incident response plan, practice it, and publicize it to your employees and colleagues [Go to **BeCyberReady.com** for guidance on how to create an incident response plan]

Be consistent with your selected telehealth platform throughout your practice

- Understand which telehealth platforms are HIPAA-compliant
- Prioritize your needs and concerns, as well as those of your patients when assessing options
- Ensure uniformity and transparency

Educate yourself about cyber hygiene basics

- Passwords: Enable multi-factor authentication and use 15+ character passphrases
- Software updates: Turn on auto-updates
- Phishing: Conduct routine phishing tests and educate your employees on what phishing attempts look like
- USBs: Use online file-sharing instead of USBs

Be aware, be prepared, and be cyber ready.

About CRI

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit www.BeCyberReady.com.