CYBER RISKS WITH TELEMEDICINE

A recent study predicted that 158 million Americans would use telemedicine by 2020 but that study was released before COVID-19 ravaged the world. It is now predicted that telehealth visits will top 1 billion this year and may be the norm post-COVID. Contributing to these numbers is the increased need for mental health visits as a result of the pandemic. Along with the safety, convenience, and reduced cost that telemedicine affords, it also brings a significant risk. Sharing electronic records of patients over third-party platforms introduces cyber exposures that could compromise patient privacy and increase the risk of HIPAA violations.

Telemedicine, although more widely used today than ever, is nothing new. The first concept of telemedicine as we know it now, dates back to an April 1924 issue of Radio News magazine. The futuristic article showed the use of television and microphone for a patient to communicate with a doctor. It wasn't until the early 1960's however, that the University of Nebraska used telemedicine to transmit neurological examinations. Other programs soon followed, but Radiology was the first specialty to fully embrace telemedicine in the 1980's. The rise of the internet in the 1990's allowed for transition to EMRs (electronic medical records) and the use of the internet became commonplace in healthcare. However, for all the convenience and cost-savings that telemedicine offers, there is also a subsequent risk of a data breach.

CYBER SECURITY AND HEALTHCARE

Healthcare has traditionally been a targeted industry for cyber breaches. Between 2009 and 2018, there have been 2,546 healthcare data breaches involving 500 or more records. Those breaches have resulted in the exposure of nearly 200 million patient records which equates to 59% of the US population. 89% of healthcare organizations have experienced a data breach in the past two years. Ransomware attacks on the industry are also on the rise. 23% of healthcare organizations have agreed to pay some form of ransom to the attackers in order to avoid downtime.

There are many different types of cyber-attacks of which healthcare companies should be aware. Here are a few examples of the most common ways data may be breached or a company's patient records compromised:

Security and Privacy Liability
Example: A hacker obtains confidential patient health information and the patient brings a claim against the provider for not safeguarding their data.

Privacy Regulations
Example: A government agency investigates a healthcare provider after a data breach is reported and issues a fine for a HIPAA violation.

Media Liability
Example: A competing healthcare facility claims that the insured's online marketing infringes on their trademark.

PCI-DSS
Example: A violation of PCI requirements which results in a cyber criminal getting access to a patient's credit card information.

Breach Event Expense
Example: An insured is contacted by a former employee that a fraudster filed a tax return in her named and accuses the company of a breach of her W2 information. The insured then hires third party specialists to investigate and determines there was a breach of over 5000 employee records.

Business Interruption
Example: A clinic has a breach that results in 48 hours of computer downtime which causes a loss of revenue.

Reputational Loss
Example: An Urgent Care Facility loses patient flow because of concerns over a possible additional breach.

Cyber Extortion/Ransomware
Example: A hacker gains access to a hospital's computer system, encrypts their information and sends an extortion email demanding payment from the hospital in order to get the decryption key.

Information Asset
Example: After a ransomware attack, a hospital is forced to incur expenses to re-create data from offsite backups.

Cyber Crime
Example: A phishing email is sent to a clinic's accounting department purporting to be a vendor and requesting re-routing of payments to a new bank account.

HOW TO PREPARE

Despite these risks, there are proactive steps that healthcare organizations can take to protect their practice, their facility, their patients and their reputation.

- **Appoint a HIPAA Security Officer** – Although the enforcement of HIPAA restrictions has been lessened during the pandemic, allowing for the use of popular telecommunication services such as Zoom and Skype, it is critical to appoint a person to keep current on all HIPAA Audit Protocol.

- **Ensure VPN Security** – The use of these networks when connecting remotely to enterprise networks will help assure that sensitive patient information is encrypted. The VPN should be functioning and up to date to mitigate vulnerabilities in the system.

- **Establish Strict Policies and Procedures Related to Data Security** – All mobile devices should be encrypted. All physicians and staff should be trained on the data security risk and the protocols to ensure the security of patient data. Lost or stolen devices such as mobile phones, laptops desktops and USB drives are the leading cause of data breaches.

- **Use Reputable Software** – There are new software technologies available due to the increased use of telemedicine. Many have yet to be tested. Any software used by a practitioner should be approved and deemed safe by their IT and Human Resources professionals.

- **Protect Against Unauthorized Access** – Hackers have become adept at capturing or guessing passwords. To prevent this, consider the use of multi-factor authentications which involves the user presenting two or more pieces of evidence to confirm their identity prior to log-in.

- **Invest in a State-of-the-Art Cyber Insurance Policy** – First and foremost, healthcare providers should make sure they are using the services of an insurance broker with specialists in cyber insurance.