MANAGE YOUR RISK

Telehealth: Cybersecurity Considerations

As defined by the Health Resources Services Administration (HRSA, 2017), telehealth is "the use of electronic information and telecommunications technologies to support long-distance clinical health care, patient and professional health-related education, public health and health administration. Technologies include videoconferencing, the internet, store-and-forward imaging, streaming media, and terrestrial and wireless communications." Because telehealth relies on telecommunications and information technology, there is an increased need to address cyber risks related to privacy and security.

Many telehealth devices require network connections, which enable them to collect information from the patient and then transmit the data to the healthcare provider. This paper intends to highlight some of the privacy and security risks related to telehealth utilization and provides some considerations for healthcare organizations to help mitigate the exposures.

Nearly 90% of healthcare organizations have experienced data breaches.

Telehealth applications can help manage and treat illness, promote the health of individuals and populations, and help control costs by providing real-time tools to promote wellness, prevent disease, and enable the home management of chronic conditions. The use of this technology, however, greatly increases the cyber exposures already faced by healthcare organizations.

Cyber Exposures in Healthcare

The Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data found that nearly 90 percent of healthcare organizations have experienced data breaches (Ponemon Institute, 2016).

- Fifty percent of data breaches in healthcare are from criminal attacks.
- Fifty percent result from mistakes, such as employee negligence, third-party incidents, and stolen computers.

According to the Ponemon Institute, this is because many healthcare organizations and their third-party business associates are negligent in the handling of sensitive patient information and "lack the money and resources to manage data breaches caused by evolving cyber threats, preventable mistakes, and other dangers" (2016).

In a clinical setting, where patient visits are face-to-face and paper-based health records are used, it is easier for healthcare providers to protect the privacy and security of healthcare information. Caregivers see each patient in a private room and patient records are locked in a secure office setting that is only accessible to authorized personnel. Many healthcare practices, however, have moved to electronic record keeping and the use of telehealth devices. It can be more challenging for providers to protect healthcare information when the information is electronic.

On the Internet, there are many ways to break into electronic systems and gain unauthorized access to a large amount of protected health information (PHI). Unfortunately, healthcare providers are not always trained adequately in protecting security and patient privacy online. The information security and patient privacy in telehealth, therefore, is at a higher risk for breaches of PHI.

- Healthcare data breaches recorded by the US Department of Health and Human Services' Office for Civil Rights show that over 189 million health records were stolen/exposed between 2009 and 2018.

Privacy Risks and Considerations

Telehealth devices and applications present significant challenges in healthcare when it comes to securing PHI and complying with HIPAA. Some privacy considerations for healthcare organizations include individual device security, access security, and HIPAA Business Associate Agreements (BAAs) and PHI use.

DISCLAIMER: This is a sample guideline furnished to you by Glatfelter Healthcare Practice. Your organization should review it and make the necessary modifications to meet your organization's needs. The intent of this guideline is to assist you in reducing exposure to the risk of injury, harm, or damage to personnel, property, and the general public. For additional information on this topic, contact your Glatfelter Healthcare Practice Representative at (800) 233-1957.

Glatfelter Healthcare Practice℠
A Division of Glatfelter Insurance Group

Device Security

Not all devices used in telehealth may be adequately protected. Even if the provider's device is secure, the patient's device may not be. Without proper monitoring services, personal computers and other personal devices may not be safe from an intrusion and the provider's device and data may be accessed through the patient's device. Providers cannot be guaranteed that patients have adequate security on their home networks. To secure telehealth devices, healthcare organizations may consider installing technical safeguards such as firewalls and intrusion detection systems (IDS) on all provider owned telehealth devices.

Access Security

Another concern is verifying the entity on the other end of a data exchange or telehealth appointment. Standard health practices are to confirm a patient's name, date of birth, and other information multiple times; however, a person who has inappropriately accessed a patient's information would be able to answer these questions. To alleviate the risks of inappropriate access, healthcare organizations may consider providing secure logins for both the patient and provider, using multi-factor authentication, and requiring information beyond PHI, such as security questions.

Business Associate Agreements (BAAs) and PHI Use

By law, the HIPAA Privacy Rule applies only to covered entities, which are health plans, healthcare clearinghouses, and certain healthcare providers. However, covered entities often use third-party services, referred to as business associates, to help carry out their healthcare activities and functions. The US Department of Health and Human Services (HHS, 2017) defines a business associate as "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity." The Privacy Rule does allow covered entites to disclose PHI to business associates; however, this is under certain provisions. The Privacy Rule requires that the HIPAA covered entity obtain "satisfactory assurances" from its business associate that the business associate will appropriately safeguard the PHI it receives or creates on behalf of the covered entity (HHS, 2017). Furthermore, the satisfactory assurances must be in writing. This may be in the form of a contract or other Business Associate Agreement (BAA) between the covered entity and the business associate.

Data Encryption

Telehealth services generate vast quantities of data. A patient may send a photo to a provider during an online consultation, or a wearable monitor may gather and store vital health information. The healthcare provider must safeguard all of this data. Data encryption using complex mathematics and encryption keys can ensure that, if an attacker gains access to any raw data, that data will be meaningless. There are three points at which data can be encrypted. Encryption of data at rest ensures that when an attacker bypasses access controls, the stored data is meaningless. Encryption of data in transit guarantees that data is meaningless if a transmission is intercepted. End-to-end encryption ensures that unencrypted information is only ever available at the two end-points and never between.

Authentication

Access to the underlying information system can be controlled using authentication and access control mechanisms, which restrict access to information based on the identity of the person accessing the device or data. There are several authentication techniques to consider. Knowledge-based authentication requires the user to know some secret information, such as a PIN, passphrase, or password, and enter the information to access the device prior to every use. Biometric authentication is another option, using something that is part of a user's attributes, such as the user's fingerprint. Multi-factor authentication combines authentication methods, for example, a knowledge-based and biometric-based authentication could be applied to a device. If an attacker breaks through the initial password, they will be upheld to the touch dynamics authentication, making it harder to access the full contents of the device. Multi-factor authentication may hinder the user's satisfaction on usability, but it will help protect the privacy and security of their PHI.

DISCLAIMER: This is a sample guideline furnished to you by Glatfelter Healthcare Practice. Your organization should review it and make the necessary modifications to meet your organization's needs. The intent of this guideline is to assist you in reducing exposure to the risk of injury, harm, or damage to personnel, property, and the general public. For additional information on this topic, contact your Glatfelter Healthcare Practice Representative at (800) 233-1957.

Glatfelter
Healthcare
Practice℠
A Division of Glatfelter Insurance Group

Distribution

Another threat in securing telehealth lies in the people who operate the devices. For telehealth to be secure business practices surrounding its use must be secure and everyone who engages with a telehealth system must be aware of the healthcare provider's policies and procedures on telehealth. It is also recommended that healthcare providers handle initial distribution of telehealth software and devices to patients in a face-to-face setting, so they can establish the identity of the patient and authenticate the device he/she is using.

Risk Considerations

Based on the security and privacy issues highlighted above, consideration needs to be given to the following issues in addition to any patient care related policies developed around a telehealth program:

- Device Security
- Access Security
- HIPAA applications for Telehealth use
- Encryption
- Authentication of users
- Distribution of Telehealth devices

Conclusion

Telehealth is rapidly developing in the healthcare industry; however, serious privacy and security risks could undermine its potential. To realize the full benefits of telehealth, patients and providers must trust telehealth systems to keep personal information private and secure. This means that healthcare organizations who work with patients and their confidential medical records must adhere to the policies, procedures, and laws designed to protect patient privacy and confidentiality and must take adequate steps in securing telehealth devices and software.

References

Health Resources and Services Administration (HRSA). (2017). Definition of telehealth. Retrieved from https://www.healthit.gov/topic/health-it-initiatives/telemedicine-and-telehealth

Office of the National Coordinator for Health Information Technology. (2016). Breaches of unsecured protected health information. Health IT Quick-Stat #53. Retrieved from https://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php

Ponemon Institute. (2016). Sixth annual benchmark study on privacy & security of healthcare data. Retrieved from https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf

US Department of Health and Human Services (HHS). (2003). Business Associates 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). OCR HIPAA Privacy. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf

DISCLAIMER: This is a sample guideline furnished to you by Glatfelter Healthcare Practice. Your organization should review it and make the necessary modifications to meet your organization's needs. The intent of this guideline is to assist you in reducing exposure to the risk of injury, harm, or damage to personnel, property, and the general public. For additional information on this topic, contact your Glatfelter Healthcare Practice Representative at (800) 233-1957.

Glatfelter
Healthcare
Practice℠
A Division of Glatfelter Insurance Group