Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Analyst Note

January 8, 2025 TLP: CLEAR Report: 202501081700

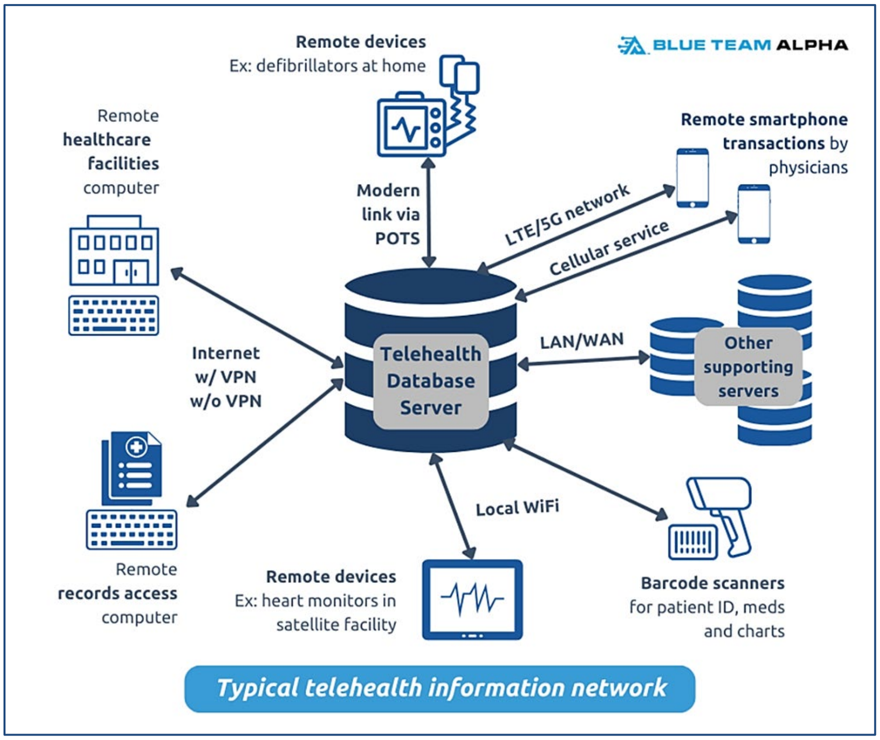
Securing Telehealth: Challenges and Solutions

Executive Summary

Telehealth leverages telecommunications and information technology to bridge the gap between healthcare providers and patients physically separated by distance. It encompasses a wide range of services, including health assessment, diagnosis, intervention, consultation, supervision, and information exchange. As telehealth evolves, its applications extend beyond traditional clinical settings, reaching patients in the comfort of their homes through virtual consultations and remote monitoring, but it also brings with it a new set of challenges, particularly in the field of cybersecurity. The integration of technology into healthcare services introduces vulnerabilities that malicious actors may exploit, and cyberattacks in the healthcare sector can lead to significant consequences. Understanding the associated cybersecurity risks is crucial for developing strategies to safeguard patient data, maintain privacy, and ensure the integrity of telehealth systems. The growing importance of cybersecurity in telehealth and the need for robust security measures is essential.

Report

Telehealth offers numerous benefits. Its convenience allows patients to receive medical consultations and treatments from the comfort of their homes, eliminating the need for travel and reducing wait time. Telehealth also enhances accessibility, especially for individuals in rural or underserved areas who might otherwise struggle to access healthcare services. It is also cost effective, reducing healthcare expenses by minimizing the need for physical infrastructure and enabling efficient resource utilization, ultimately leading to lower costs for patients and providers.


BLUE TEAM ALPHA
Remote devices
Ex: defibrillators at home
Remote healthcare facilities computer
Remote smartphone transactions by physicians
Modern link via POTS
LTE/5G network
Cellular service
Internet w/ VPN w/o VPN
Telehealth Database Server
LAN/WAN
Other supporting servers
Local WiFi
Remote records access computer
Remote devices
Ex: heart monitors in satellite facility
Barcode scanners for patient ID, meds and charts
Typical telehealth information network

Source: Blue Team Alpha

As telehealth becomes an integral part of healthcare, ensuring robust cybersecurity is key to protecting patient data, complying with regulations, and building trust in these services. The unique cybersecurity challenges facing telemedicine today underscore the importance of adopting stringent security measures to protect the sanctity of this vital service. However, the very features that make telemedicine platforms so appealing also make them attractive targets for cybercriminals. According to healthcare data breach statistics, cybercriminals illegally accessed over 342 million patient records between 2009 and 2022. Patient data in telehealth includes highly sensitive information such as medical history, personal identification details, and financial information. Any breach can lead to severe consequences, including identity theft, financial fraud, and erosion of patient trust.

Challenges of Telehealth

While revolutionary in healthcare delivery, telehealth systems face a spectrum of cyberthreats that require diligent cybersecurity measures to safeguard patient information and maintain service availability. Understanding the major types of attacks is crucial for devising comprehensive defense strategies tailored to the unique challenges posed by telehealth platforms. The impact of these attacks on telemedicine platforms cannot be overstated. The real-time nature of telemedicine, coupled with its requirement for high availability, means that any disruption can have immediate and severe consequences. The vulnerabilities inherent to these systems, especially when compared to more traditional healthcare IT infrastructures, exposes them to a range of cyberattacks, such as:

- *Data Breaches:* Occur when unauthorized individuals gain access to sensitive patient data stored on telehealth platforms. The stolen data can include personal identification information (PII), medical history, and financial details.
- *SQL Injection Attack:* Occur when an unintended query is entered into a database application. This is particularly dangerous for telemedicine platforms because it can lead to unauthorized access to sensitive patient data stored in the database.
- *Cross-Site Scripting (XSS) Attack:* Involves injecting malicious scripts into content from otherwise trusted websites. For telemedicine platforms, this could mean the unauthorized execution of scripts in a user's browser, compromising the integrity of the platform and the confidentiality of patient information.
- *Session Hijacking:* In this type of attack, the cybercriminal exploits the web session control mechanism to steal confidential information. Given the real-time nature of telemedicine consultations, session hijacking can disrupt ongoing care sessions or allow unauthorized access to personal health records.
- *Ransomware:* Malicious software that encrypts data on healthcare providers' devices, making telehealth systems and patient records inaccessible until a ransom is paid. Ransomware attacks can severely disrupt telehealth services.
- *Phishing Attack:* Involves cybercriminals sending deceptive emails or messages that appear to be from legitimate healthcare providers or telehealth platforms. These messages often contain malicious links or attachments designed to steal sensitive information such as login credentials, personal details, or financial data.
- *Distributed Denial of Service (DDoS) Attack:* Involves overwhelming telehealth platforms with a flood of internet traffic, causing them to slow down/crash. These attacks can disrupt telehealth services, making it difficult for patients to access care.
- *Increased Risk of Insider Threats:* Insider threats, whether intentional or accidental, pose cybersecurity risks. Unauthorized access, mishandling of patient data, or negligence in adhering to

cybersecurity protocols by healthcare staff can compromise the confidentiality and integrity of telehealth systems.

There is also the issue of data privacy and confidentiality. In telemedicine, the main cybersecurity concern is the stringent protection of patient data, which is subject to strict regulations, most notably, HIPAA. Medical records are a goldmine of personal information, making them a prime target for cybercriminals. Unlike physical records, which require direct human access, digital records can be accessed remotely if they are not properly secured. The risk extends beyond unauthorized access. HIPAA-compliant hosting is a significant factor in this regard, as modern healthcare facilities also must be certain about the reputability and trustworthiness of their hosting provider. Likewise, Advanced Persistent Threats (APTs) and Man-In-The-Middle (MITM) attacks, where attackers insert themselves into the communication channel between patients and healthcare providers, pose a substantial risk. These sophisticated attacks can bypass traditional security measures, intercepting data even when encryption is in place.

Solutions: How to Secure Your Telehealth Environment

For telehealth to be effective, patients must trust that their sensitive information is secure and that their privacy is respected. When patients are confident that their data is protected, they are more likely to engage with telehealth services and share necessary information openly with healthcare providers. This trust enhances the patient-provider relationship, improving the overall quality of care and patient satisfaction.

- **Adopt A Zero-Trust Architecture for Telemedicine**. Adopting a Zero Trust architecture, which operates on the principle of "never trust, always verify," offers a promising defense strategy for telemedicine platforms. This approach assumes that threats can originate from any location—inside or outside the network—and therefore verifies every access request as if it originates from an untrusted source.
- **Utilize Multi-Factor Authentication.** Multi-Factor Authentication (MFA) enhances security by requiring users to provide two or more verification factors to gain access to telehealth systems. Healthcare providers should implement MFA for all access points to telehealth platforms.
- **Perform Regular Software Updates.** Cybersecurity is a constantly evolving field with new threats emerging regularly, and often increasing in scope and potential risk of harm. As a result, telemedicine platforms and the devices used to access them must be kept up to date with the latest security patches and software updates. These updates often contain fixes for security vulnerabilities and if left unpatched could be exploited by cybercriminals.
- **Training and Awareness.** Human error remains one of the largest vulnerabilities in cybersecurity, so educating both healthcare providers and patients about the importance of cybersecurity measures is crucial. Implement core competency training for all telehealth providers and users. Healthcare practices are only as secure as the weakest link, so educating staff on telehealth safety and cybersecurity best practices is vital.
- **Adhere to Legal and Regulatory Compliance.** Adhering to legal and regulatory requirements is essential for telemedicine platforms to safeguard sensitive patient data while also ensuring compliance. Compliance protects patient information while shielding telemedicine providers from legal and financial penalties. Staying informed and up to date with these regulations ensures that telemedicine services can provide secure and lawful care, maintaining trust and credibility in the digital healthcare ecosystem.
- **Invest in an Encrypted, Password-Protected Platform,** as well as a service agreement that ensures

maximum security. Encryption is vital to securing patient data and can help healthcare organizations comply with regulations, enable secure data sharing, and reduce the risk of costly data breaches.

  - *Encrypted data at rest:* Encrypting data at rest ensures that all patient data is stored securely in the cloud or on a device. This prevents hackers from acquiring access to the data without decrypting it first.
  - *Encrypted data in transit:* Data that is transferred over networks should be encrypted to avoid being intercepted before reaching the intended recipient.

- **Share Updated Security and Privacy Practices with the Patient.** Notifying patients of updated security and privacy practices provides them with necessary disclosure and peace of mind.
- **During Telehealth Sessions:**
  - Use a private space and limit the number of people participating in the session. Conduct telehealth sessions only in secured spaces with private Wi-Fi and no public entry, preventing unauthorized online and physical access. Ensure session access is limited to only personnel directly involved in the patient's care and those the patient has authorized.
  - Never leave systems logged in. Close or sign out of applications, and turn off all monitors, microphones, and cameras once the telehealth session is complete.
  - Secure any notes, electronic devices, storage media, and written materials when not conducting patient sessions. Try to avoid saving patient data on shared or personal devices,

Analyst Comment

The integration of telemedicine into the healthcare sector is a testament to the ongoing technological advancement and innovation encountered in recent years, but the importance of cybersecurity cannot be overstated. The risks associated with telemedicine are significant, but with careful attention to data privacy, communication security, and regulatory compliance, these dangers can be mitigated. The future of telehealth security will be characterized by a combination of technological innovations, user-focused education, standardized protocols, and strategic integrations with emerging technologies. As the telehealth landscape continues to mature, these developments will play a pivotal role in fortifying the resilience and trustworthiness of telehealth systems.

References

13 Steps for Securing Patient Privacy While Using Telehealth
https://www.telementalhealthtraining.com/telehealth-explorer/13-steps-for-securing-patient-privacy-while-using-telehealth

Telehealth Privacy and Security Tips for Patients
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/telehealth-privacy-security/index.html

The Rising Importance of Cybersecurity in Telehealth
https://blog.charlesit.com/the-rising-importance-of-cybersecurity-in-telehealth

Safeguarding the Future: Navigating Cybersecurity Challenges in Telehealth
https://blueteamalpha.com/blog/cybersecurity-challenges-in-telehealth/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback