Telehealth Security

by Capella Healthcare

WHAT'S COVERED

In this lesson, you will learn about different types of security related to telehealth and information technology (IT). Specifically, this lesson will cover:

1. Logical and Physical Security
2. Network and System Security
3. Mobile Device Security
4. Data Security and Privacy

1. Logical and Physical Security

Logical security covers things that can be visualized but are intangible, including data, applications, and information.

Physical security covers things you can see, feel, or touch, including phones, tablets, paper, or computers. This type of security includes being mindful of unauthorized people looking over the healthcare personnel (HCP)'s shoulder to observe the entry of passwords and other authentication, PHI, or other sensitive data (known as “shoulder surfing”).

Logical Security	Physical Security
Passwords Malware protection Control of access to ePHI	Protection of physical forms of PHI while traveling through opaque cover sheets and envelopes Monitor positioning to avoid unauthorized viewing Use of headphones to avoid unauthorized hearing

According to the Center for Internet Security (2020), a threat actor is a person or group that has the potential to do harm to an organization, its information system, people, or data. This entity can impact the HCP in the form of intercepting communication (network) through inefficient encryption, successful phishing attempts through email and/or text message, and/or modifying/destroying data.

2. Network and System Security

Included in system security are considerations needed to protect mobile (tablet, laptop, phone) and stationary (desktop computer, printer, fax, scanner) devices. Security requirements to ensure smooth processing and functioning of the system include updating software as manufacturer patches become available, malware protection with up-to-date signatures and application revisions, and managing mobile devices. Stationary systems (desktop computers, printers, scanners) have similar protection requirements.

Email is used heavily in interactions between the HCP and the patient. Free email such as Yahoo or Hotmail may not have the security appropriate for the protection of PHI and other sensitive data. The HCP should avoid using this type of email solution, defaulting to send messages through the EHR, corporate email, or approved telehealth medium.

With email and text messages on mobile devices, threat actors may send messages that appear to come from valid sources (e.g., management, credit cards or banks, family). This is where vigilance in managing systems and paying attention to communication methods are key. Refer to Data Security and Privacy for helpful tips on addressing communications security.

3. Mobile Device Security

Mobile device security is important for managing the security and privacy of data. The following are security best practices for mobile devices per ONC (2020) for addressing the security of data and cellular systems. They are to:

- Use secure wireless network settings
- Use complex passwords or other authentication for access to the device and applications
- Use encryption (method to hide data or make it unreadable to the naked eye)
- Use a remote wipe or disable features in case the device is lost or stolen
- Be mindful of mobile applications and permissions given
- Disable file sharing features
- Enable firewall or other security software (Virtual Private Network, malware protection)
- Keep watch of physical security of the device, data entry, and telehealth consultations

Mobile devices will use both cellular and wireless networks to enhance communication capabilities. Many mobile devices use a wireless home or office network. These networks are important vehicles to use to access various system applications, access EHR and CDS systems, and conduct telehealth consultations. Open or public wireless access points for WiFi can cause data loss or integrity concerns due to minimal security settings. Threat actors can mimic these WAPs, setting a “trap” for users to steal information or credentials.

4. Data Security and Privacy

Health data will need to be protected in storage (database, EHR), traversing across the network (email, entry into the EHR across the network), or actively in use by patients’ wearable health technology (e.g., blood sugar monitors). Threats and vulnerabilities with data stored, in transit, and in use include:

- Interception attacks (man-in-the-middle)

- Out of date software (corrupt data)
- Email impersonation (phishing)
- Loss due to lost or stolen devices

Ways to protect data in transit include encryption, password management, malware protection, and the use of a secure medium for telehealth.
For email and text messages, the following are key points to reduce the risk of malware injection with devices:

- Do not click links in unsolicited emails or text messages.
- Encrypt emails and data to protect PHI in various states.

Approved telehealth technology methods have a level of acceptable cybersecurity measures for the respective systems. In addition to technology, there should be a signed business associate agreement that establishes requirements for the technology provider to have processes and procedures under the HIPAA Privacy and Security Rules.
Approved telehealth technology communication methods include:

- Skype for Business / Microsoft Teams
- Updox
- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet
- Cisco Webex Meetings / Webex Teams
- Amazon Chime
- GoToMeeting
- Spruce Health Care Messenger (HHS, 2020)

Unapproved versions of telehealth methods may not have appropriate security settings. These versions also have privacy implications due to the permissions required, such as those regarding access to a camera or microphone, contacts, and other applications. The same privacy issues occur with the use of unsigned mobile applications which are not developed or approved for telehealth use by the device manufacturer.
Unapproved telehealth technology communication methods include:

- Free conference call
- Free versions of Zoom
- Facebook Messenger (HHS, 2020)

HINT

The HCP can refer to their HIPAA Privacy and Security Officer for further information on other approved sources for telehealth engagements.

Authored by Cindy Ebner, MSN, RN, CPHRM, FASHRM and Tamika K. Williams, MSIT.CS, CISM, CISSP, CAP, SSCP, HCISPP, COBIT 5 Foundation/Implementation

Support

If you are struggling with a concept or terminology in the course, you may contact **TelehealthSupport@capella.edu** for assistance.

If you are having technical issues, please contact **learningcoach@sophia.org**.