CALIFORNIA TELEHEALTH RESOURCE CENTER

Part of OCHIN

Frequently Asked Questions (FAQ) for Patient – Virtual Care Security

1. How do I know my video visit will be secure?

It is essential to know that your health care provider has a responsibility to protect your privacy during a video encounter. One of the most important things the Health Insurance Portability and Accountability Act (HIPAA) did was to require the protection and secure handling of certain information, known as Protected Health Information. For example, your health care provider must have systems in place to ensure that only authorized individuals have access to your health information. This is true whether the information is on paper or in a computer system. HIPAA regulations also apply to any information transmitted over the internet, including video visits.

To comply with HIPAA, your health care provider must use a virtual solution that meets HIPAA's strict standards. Please contact your health care provider with any questions or concerns about the privacy and security of information shared during your telehealth session.

2. What are the safeguards of virtual care?

HIPAA requires that providers integrate encryption and other safeguards into their interactions with patients. All medical professionals or health care organizations providing remote services to patients in their homes or in community centers must comply with HIPAA guidelines. HIPAA privacy and security regulations provide protections for identifiable health information. HIPAA's Privacy Rule establishes limits on the use and disclosure of identifiable health information;, and its Security Rule establishes technical, physical, and administrative safeguards that protect identifiable electronic health information. For example, encryption of data at rest and in transit is an "addressable implementation specification" under the Security Rule. This means that HIPAA-covered entities are expected to encrypt unless it is not "reasonable and appropriate" to do so. In addition, the regulation states that providers are required to adopt identity management protocols and access controls.

3. What are the risks of using public Wi-Fi during my telehealth visit?

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, and other public places are convenient, but often not secure. Needing a password to log in doesn't necessarily mean your online activities are encrypted. Public Wi-Fi can leave you vulnerable for different reasons. One has to do with the encryption protocol used by some wireless networks. Another involves the possibility of joining a fake or rogue Wi-Fi hotspot. Using public Wi-Fi hotspots to conduct virtual visits is not recommended. Consider using your mobile data instead of Wi-Fi as an alternative. (Note: You may be charged for this data use based upon your cellular plan).

4. What are some common security threats?

- **Phishing attacks**
  Phishing attacks occur when an attacker pretends to be a trusted contact., A phishing attempt may entice a user to click a malicious link; download a malicious file; or provide access to sensitive information, account details, or credentials.

- **Malware attacks**
  Malware encompasses a variety of cyber threats, including Trojans and viruses. All involve malicious code that hackers create to gain network access, steal information, or destroy data on computers. Malware usually comes from malicious website downloads, spam emails, or connection with other infected devices.

- **Ransomware**
  Ransomware is a specific type of malware that infects and restricts access to a computer until a ransom is paid. Ransomware is usually delivered through phishing emails and exploits unpatched vulnerabilities in software.

- **"Man in the Middle" (MitM) attack**
  In this case, an attacker establishes a position between the sender and recipient of electronic messages and intercepts those messages, perhaps changing them in transit. The sender and recipient believe they are communicating directly with one another.

5. How does Antivirus and Anti-malware software protect my computer?

Benefits of antivirus and anti-malware software

- Detects and protects against malware, viruses, and other harmful software in real time
- Contains proactive anti-ransomware and anti-exploit detection and response components
- Blocks hacking and phishing attempts
- Offers flexibility through manual and scheduled scan modes
- Provides a layered approaches to securing your computer

6. What are the benefits of using a firewall during telehealth visits?

Firewalls protect against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. They can be configured to block data from certain locations (e.g., computer network addresses), applications, or ports while allowing relevant and necessary data through.

7. What is malware and how do I get rid of it?

Malware is short for *malicious software*—software used by hackers to impair your device's function, steal data, or even gain control of the device itself. Typically, malware is downloaded unintentionally when an unsuspecting user opens an infected file or visits an infected website. Once it's on your computer, it launches a specific kind of attack based upon its design. For example, keyloggers record each keystroke and report this information to hackers, who look for usernames, passwords, and other sensitive credentials. Trojans masquerade as useful or benign software—for example, fake antivirus software or games. This tricks users into opening the Trojan, thereby granting access to system files, or facilitating download of more malware.

You can protect your computer against malware by installing antivirus software and running routine scans. If your computer is running slowly or taking unusual actions (such as "reminding" you to download strange software), it may be infected with malware. Run an antivirus scan to check for, identify, and remove malware from your device.

8. Why are strong passwords important and how do I create one?

It's important to develop strong, unique passwords across all your online logins and accounts, not just those used for telehealth. Strong passwords are important for keeping your online accounts and personal information safe from cyber criminals. Enabling two-factor authentication provides an additional layer of security.

Creating a strong password:

Step 1: Use five different words relating to a memory that is unique to you. (e.g., Learntorideabikeatfive)

The longer a password is, the harder it is to guess. Be sure not to use personal information such as your name, national registration identity card (NRIC), birthdate, or other information that can be easily obtained via online search.

Step 2: Use uppercase and lowercase letters, numbers, or symbols to make it even harder to crack. (e.g. LearnttoRIDEabikeat5)

Remember to keep it random by ensuring that your password does not have a predictable pattern. This means it should be difficult for others to guess, even with special tools. Some examples of obvious patterns include:

- Using common phrases (e.g., maytheforcebewithyou)
- Capitalizing the first letter of the password (e.g., Livelongandprosper)
- Adding a number at the end (e.g., qwerty1)
- Replacing a letter with a number or symbol (e.g., p@ssw0rd)

Now that you have successfully created a strong password, enable 2FA. This stands for two-factor authentication, which adds an extra layer of security to your account.

9. How does updating my internet browser protect my computer?

Updating your internet browser provides superior protection against scams, viruses, Trojans, phishing attacks, and other threats. It can also resolve security vulnerabilities present in your current browser. Many browser updates are issued to combat these exact problems. For optimum safety and security when using the internet, always run the latest version of your chosen browser supported by your operating system.

11. What scams should I be aware of?

Don’t open suspicious attachments or click unusual links in messages. They can appear in email, tweets, posts, online ads, messages, or attachments. Sometimes they also disguise themselves as known and trusted sources.

Know how and when you will be contacted for your telehealth visit, or to obtain any follow-up information. If you receive a suspicious call or email about your telehealth visit, contact your health care provider. Better safe than sorry.

12. What is phishing and how do I avoid it?

Phishing refers to any type of digital or electronic communication designed for malicious purposes. It is a type of social engineering attack that uses impersonation and trickery, often persuading an innocent victim to provide private information such as login credentials, bank account information, social security number, or other sensitive data.

A cyber criminal’s goal is to use this information to defraud the victim in some way—stealing money, taking over one or more accounts, creating fraudulent new accounts, or running up credit card charges. In some cases, the attacker’s ultimate goal is to take over a victim’s device using malware. The perpetrator may also wish to gain access (through the victim) to other valuable resources including enterprise networks, systems, data, or intellectual property.

Recommendations for individuals:

- Be cautious about all unsolicited email and text messages.
- Hover over embedded links (without clicking) to reveal the actual URL and compare it the link that's shown.
- Never click embedded links, even if you think they're trustworthy. Instead, use your browser to search for the correct URL.
- Never open attachments of any kind in unsolicited email. In email from known senders, separately verify attachments before opening them.
- Please contact your health care provider about emails or text messages with embedded links or attachments to validate this information and ensure your privacy is protected.
- Use antivirus and anti-malware on your personal devices and keep them updated.
- Use multi-factor authentication on every account that offers it. This helps prevent cyber criminals from accessing your accounts.

13. How should I backup my data?

You can make and store regular backup copies of all valuable information on your device by using either external media or a cloud-based service. The process can be simplified and automated by using a third-party backup application. Be sure to encrypt your backup to protect the confidentiality and integrity of your information. Data backups are important to minimizing negative outcomes if data is lost, corrupted, infected, or stolen.

14. What items should I remove before my telehealth visit?

Before beginning a conversation with your health care provider, make sure you remove items that are not needed to discuss your health concerns. Technology devices not being used to contact your health care provider should be removed to avoid capturing potentially sensitive information. Some examples are home security cameras or voice assistants.