TELEHEALTH: WORKING SECURELY with PHI

Providing excellent service is increasingly important as our clinics rapidly adjust to new business processes. The CEHS IT and SCCE Compliance Offices would like to ensure data protection controls are part of this new process implementation.

Documentation

With a signed and dated Telehealth Attestation Form, you may provide telehealth services on-site, in either a tele-suite or therapy room in the SCCE building. Exceptions to this policy are granted only under extenuating circumstances and require a properly approved Telehealth Exceptions Form. Before providing telehealth services, take a moment to read and understand the necessary information resources (below) for proper tele-work.

Links to Related Documents: Telehealth Policy 119 | Telehealth Operation Procedures | Pre-Teleservice Checklist | Telehealth Attestation Form | Telehealth Exceptions Form | Other CEHS Privacy and Security Policies and Procedures

Approved PHI Systems

Point and Click PnC and HIPAA Box folders (storage and processing)
Virtru (email)
Zoom and IVS (video conferencing or telehealth)

Note
(1) The storage of PHI must be on SCCE-approved platforms—PnC and Box HIPAA folders. PHI must not be downloaded to devices.
(2) Access to PnC must be on a Sorenson-Issued and Maintained device. Audits will be performed to ensure compliance with PnC access.

Devices

Sorenson-Issued and Maintained Device
Using a Sorenson-issued and maintained device, configured to meet HIPAA security requirements, is always the best alternative for conducting clinic work.

CEHS-Approved Device
If the use of a Sorenson-issued and maintained device is not available, you are required to use a CEHS-approved device. This means the device complies with CEHS IT standards for PHI and is verified compliant by a CEHS IT staff member before use. CEHS IT standards include (at a minimum): unique account username and strong password, device encryption, anti-malware (Windows), up-to-date operating system and software, and USU VPN client.

- Password Composition Requirements
  - Long – use least 12 characters
  - Random – use random words, characters, and number combinations
  - Unique – do not use this password on other accounts
  - Private – do not share the password
- If you must use a shared computer, you must have your own username and a strong 12-character password (same as above).
- Family and guests must understand they cannot use your work device. They could accidentally erase, modify, or infect the device.

Required Software for PHI devices

- Encryption: Bitlocker (Windows) and FileVault 2 (Mac) are the common device encryption software.
- Updated Operating System: see Best Practices for Personal Computers (below).

For details on minimum requirements, please view Best Practices for Personal Computers (Windows and MAC).

Connections

Virtual Private Network (VPN)

All PHI-related work must be conducted through a VPN connection, as it provides a secure, remote connection to the USU network by providing an encrypted stream between your computer and campus.

With a secure internet connection, authorized users can access the university network from remote locations, such as the home office or public locations (e.g., conference venues and coffee shops). If you are using public WiFi (e.g., xfinity hotspots) or personal/home WiFi that doesn't have at least WPA2 security enabled, a VPN is mandatory.

VPN Instructions

Step 1: Download the USU VPN Client for your operating system and follow USU step-by-step instructions.

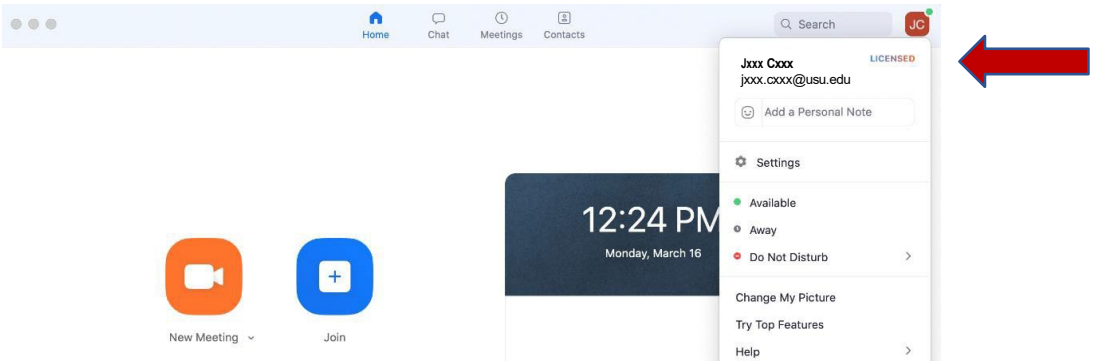
Step 2: After the Cisco AnyConnect client is installed, follow the instructions for the USU Staff VPN. The Staff VPN adds an additional layer of security.

Telehealth Tools

Zoom

Zoom has two user types: Basic and Licensed.

A Zoom Licensed Account must be used for HIPAA compliance, unless otherwise approved through the exception request process. Please verify the licensing each time you open the Zoom application, as shown below. If the word "Licensed" appears after your profile name, you are in a secure Zoom session. If the word "Basic" follows your name, STOP, you are not using the HIPAA-compliant version of the platform.



Before using Zoom for patient interaction, please test your audio and video connection at zoom.us/test. In addition, check your bandwidth to ensure your connection speed is adequate. Links such as speedtest.xfinity.com, speedtest.att.com, or fast.com will quickly check your bandwidth.

A Zoom video conference requires up to 3 Mbps of download 3 Mbps of upload. For more information, please visit Zoom bandwidth requirements.

If your Zoom meeting is choppy or pixelated, try these tips…

- Move your laptop closer to your wireless access point or router.
- Plug your computer directly into your router via a wired Ethernet jack connection, instead of the WiFi connection (newer Macs and Chromebooks will need a dongle/adapter to use the jack). This should dramatically improve dropouts and speed issues.
- Close other non-essential activities while you are working, especially video streaming or gaming.
- Limit others using your router from video streaming or gaming.
- If using a laptop, plug the laptop into wall power. Battery use can adversely affect video quality.
- Turn off your Zoom video, using just audio, if you are experiencing quality issues during a video conference.
- Reboot your router according to the instructions from your Internet Service Provider (ISP).

Additional Security Measures

Inactivity Screen Lock. Configure your computer screen to lock automatically after 5 - 15 minutes of inactivity.

Privacy Screens. Use privacy screens on your devices if there is any chance of spying eyes.

Headsets. Use a headset as an added data privacy measure.

Remove Smart Speakers. To ensure that Zoom sessions or other sensitive verbal conversations stay private, unplug or remove the smart speakers from your home office. Studies have shown that smart speakers are always listening, so they are able to detect the key phrases they are programmed to recognize. This means they will pick up any conversations or sounds in range.

Physical Security. Ensure your work area is secured.

Support

For help on IT-related topics, please contact Don don.gustafson@usu.edu or Jordan jordan.robertson@usu.edu.

For updated information, review the Working Remotely information available under the USU Information page, particularly in light of the COVID-19.