HIPCO Ancillary Review Aid:

Computer Device Guide for Research

Overview

All computer devices used to store, view, handle, or process Protected Health Information (PHI) need to be HIPAA compliant, including devices used to access data within BOX, REDCap, or HST servers. HIPAA compliant devices are all Health Sciences Technology (HST) managed, so if the study team needs to view or edit a data file containing PHI, they need to do that from an HST managed device or one of the HST provided alternatives. *HIPCO will make all determinations if health data is or is not considered PHI.*

Frequently Asked Questions

- **Do I need a HIPAA compliant device for my study?** *Does this study involve Protected Health Information as outlined in the deidentification guide?* If **yes** - You need a HIPAA compliant device to handle this data. If **no**, and all data is fully deidentified according to the deidentification guide, a HIPAA Compliant device is not required, but highly encouraged. **Note that Study IDs that can be linked to participant PHI are a HIPAA identifier and are not inherently deidentified according to HIPAA.*
- **Does this apply to me if my study team lies completely outside of the Healthcare Component?** Maybe. If the study team is receiving PHI (including Limited Datasets) from a covered entity (Healthcare provider, Health plans, a Healthcare Clearinghouse, or an organization with whom the University has a BAA), then HIPAA may apply and all device and data storage compliance requirements would be needed.
- **Can I use a Fairview managed device or UMP managed device to conduct my HIPAA protected study?** Yes, the standard Fairview and UMP managed devices are considered HIPAA-compliant and are approved for use with research data containing PHI.

HIPAA Compliant Computer Device Options

- **HST Managed Laptop or Desktop**

  Health Science Technology (HST) offers HIPAA compliant devices that are approved to handle PHI. For help in obtaining a HST Device or for more information on this topic, please visit the HST Webpage for support.

  - **Fairview or UMP managed Laptops or Desktops are approved to handle PHI**

- **Remote Access from Non-HST devices**

  Non-HST managed computers, including personally owned computers, may be used to access PHI only when combined with the Secure Computing Environment (HST-provided Remote Desktop service + VPN) or if all data access occurs within the AHC-IE Data Shelter.. Otherwise, no PHI may be handled, viewed, or copied with non-HST managed computers. Individuals are responsible to ensure that non-HST managed computers are free of screen recorders, keyloggers, or anything that might put PHI at risk. Individuals must follow University Policies and any guidance or restrictions specified by the applicable Remote Access service..

Available Services

- Secure Computing Environment (Remote Desktop to HST device + VPN)*
- AHC-IE Data Shelter**

*****NOTE:** The VPN alone is not enough to ensure compliance. The VPN must be used in conjunction with a Remote Desktop Connection to a HST computer. HST can assist in setup for this function.*
******NOTE**: If data will be extracted from the Data Shelter, device compliance requirements apply . CTSI can assist in consultations for this service.*

When using the Secure Computing Environment:

Please copy and paste the following into the protocol (insert under subsection “Other Non-HST Managed Devices”): *Personal computer devices will be used when connected to the HST Secure Computing Environment (Remote Desktop connection to a HST device and VPN). No data will be accessed without use of the SCE or stored locally on personal computer devices.*