RESEARCH NEWS
Washington University in St. Louis

Policies and Requirements for Remote Work at Washington University School of Medicine

From the HIPAA Privacy Office and Information Security Office

As we prepare for contingency work arrangements in response to COVID-19, we must also focus attention on ensuring the continued security of Protected Health Information **(PHI).** All Washington University HIPAA and Information Security policies and procedures, including those for handling physical and electronic PHI, remain in effect as if the employee was working onsite at the university.

Protecting Discussions Involving PHI
If you must discuss protected health information with co-workers, other health care entities, vendors, patients, and others, employees need to identify a location within their home, which will allow for this communication to occur privately and securely. Consider modes of non-verbal communication such as the chat tools in Microsoft Teams.

Protecting Paper-Based PHI
Please limit the removal of paper-based PHI from the university workspace whenever possible. Instead, consider secure electronic alternatives to transporting paper, such as scanning the documents before working from home and storing them in a secured network drive or WUSTL Box.

If paper-based PHI must be transported to the home environment or created at home, the employee is obligated to ensure the physical security of the PHI by following the "2-key concept". The "2-key concept" means PHI at rest is stored in a locked "container" within a locked environment. For example, PHI can be stored in a locked bag and the locked bag stored within a locked home.

Paper-based PHI no longer needed for the intended purpose should be returned to the university for proper disposal in the university approved Shred-It containers. Employees are prohibited from disposing of documents utilizing home disposal methods, even if the documents are shredded first.

What Technologies are HIPAA Compliant?
The link below has a listing of approved services for use with HIPAA information.
informationsecurity.wustl.edu/services/secure-storage-and-communication-services/

Chat and Collaboration
Please use Microsoft Teams or Zoom to have online meetings or chat discussions concerning patient information. Do NOT use mobile device text messaging to communicate any identifiable patient information.

File-Sharing
Departmental file shares through WashU VPN, WUSTLBox, and WashU Microsoft OneDrive are approved to share HIPAA related files. When using these services, please be aware that you must save the document in these environments and not your local computer.

Remote Access
The Medical School VPN and departmental Citrix services are the approved methods for remotely connecting to the School of Medicine network. Please be sure you use the Medical School VPN when connecting from a remote location e.g., Starbucks, public library, or other open-access WiFi hotspots. Please refer to the guidance above for approved systems for file-sharing and collaboration in the event that the VPN connection is unavailable.

Use of Personal Device
If you have a work-issued laptop or tablet, it should be your method for conducting medical school business while working remotely. If you must use a personal device, the device must be compliant with the university's Personal Device Security Policy.

School of Medicine
As required by state, federal, and industry regulations, WashU community members must connect to the WashU network with personal devices that are encrypted and able to receive vendor updates and patches. These protections aim to reduce the risk of WashU School of Medicine information being stored or accessed from devices that may not be able to secure the information. Minimum requirements are provided for Windows and Mac devices in the Personal Device Security Policy. Other vendor devices are acceptable as long as they are able to meet these requirements.

WashU device owners will not store protected health information on personally owned devices. If there is a need to store protected health information on a personally owned device, it must be encrypted to comply with the WashU Encryption Policy. Failure to comply with the Encryption Policy will result in sanctions under the WashU Policy on Sanctions for Non-Compliance with HIPAA Policies.

WashU reserves the right to update and require any additional controls for personal devices based upon the risk to the WashU network or environment.

Password and Device Protection
If you are using a shared family device to conduct medical school business, you ***MUST*** logoff and disconnect from all university resources before allowing others access to this device. When away from the device, the screen should be locked to prevent unauthorized access.

Email Security
With the increased concern about COVID-19, there has been an increase in phishing attacks to attempt to gather your credentials or access your computer. You should never provide your university user id and password to anyone through email or phone call. Additionally, please refrain from selecting any options to stay logged in to your email accounts on computers that are shared or being used for remote work.

Notification of Security or Privacy Incidents
Please remind employees of their continued requirement to report Information Security and Privacy related incidents immediately. For more information on the reporting requirements, please see the Information Security and HIPAA Privacy Office websites.

Thank you in advance for your assistance in protecting our patients' privacy during these challenging times. If you have additional questions or concerns, please contact the Information Security Office (infosec@wustl.edu) or HIPAA Privacy Office (hipaa@wustl.edu).