COLUMBIA | COLUMBIA UNIVERSITY IRVING MEDICAL CENTER

PRIVACY OFFICE

Protecting Sensitive Information

Physical Privacy Guidelines

With new technology and changing business practices, we find more of our Columbia workforce members working remotely. While there are benefits to remote work, there are also protections that must be in place to ensure compliance with federal and state patient privacy regulations.

This guidance document provides best practices to protect patient confidentiality while working in the office or remotely.

WORK ENVIRONMENT

- Have physical safeguards (e.g., privacy screen filters for monitors) in your work area to ensure electronic Protected Health Information (ePHI) cannot be viewed by others
- Your dedicated home workspace should be in a private area, for confidential conversations
- Use earphones or a headset when appropriate
- Lock your computer screen when you step away from your computer so that unauthorized persons cannot access/view information on your workstation
- All electronic devices must be secure from theft and other unauthorized access and use at all times. Avoid having these devices in areas that can easily be accessed by others.
- Avoid printing PHI or other sensitive information whenever possible.
- If patient information must be printed, storage of paper PHI in your home or in the office must be in a secure filing cabinet; do not leave documents unattended or accessible for potential unauthorized viewing.
- Securely discard (e.g., shredder, Shred-it bin) paper documents that contain PHI as soon it is no longer needed.
- When transporting PHI, including ePHI, it must be for approved business purposes and it cannot be left in a locked car, in checked luggage on a plane, etc., and must be in your direct physical possession.

TRANSMISSION OF PHI

- Do not use unapproved text messaging services (e.g., iPhone text messaging, Facebook Messenger, WhatsApp) to communicate patient or other sensitive information. Epic Haiku and Rover provide secure messaging that may be used to communicate with care team members, and the care team should utilize CONNECT to communicate with their patients.
- For emails sent to external email addresses, double check the email address to ensure the recipient is correct and use #encrypt in the Subject Line for emails containing PHI or other sensitive information
- Do not include patient identifiers (e.g., name, MRN, DOB) in the Subject Line of an email

DEVICES

- Do not allow family, friends, roommates, etc., to use devices that are used for work. If a home computer must be shared, individuals should have their own login credentials, you must log off after each use, and passwords should not be saved for access to work-related applications.
- PHI should not be copied to external media (e.g., flash drives and hard drives). If it is part of your approved job function, then only download PHI when necessary to an approved storage drive (e.g., P: drive or other shared CUIMC network drive)
- If you use a personal device to perform Columbia job functions, you are obligated to comply with all CUIMC IT security policies and requirements
- Make sure your wireless router is encrypted and that you change the default password
- Disconnect from the CUIMC VPN when you are done working
- Turn off the Alexa/Google device microphone when you are discussing confidential patient information

REPORTING

- All Columbia workforce members are required to immediately report any privacy issues or concerns to their supervisor or the Privacy Office at privacy@cumc.columbia.edu
- Information security questions or issues should be reported to the Information Security Office at security@cumc.columbia.edu

RELATED RESOURCES

- CUIMC IT: Remote Work
- CUIMC IT: Are you ready to work remotely?
- Columbia HR: Telecommuting Policy | University Policies
- CUIMC HR: Managing Remote Teams--Best Practice Guide