MEDICAL CENTER INFORMATION

VUMC COMPUTERS AND CLINICAL APPLICATIONS

General Information

- Clinical Workstations (CWS) provide staff access to VUMC applications.
- Icons for these applications and others are located on the desktop.
- The Digital Library Page at https://www.library.vanderbilt.edu/biomedical// has other available sources.
- All computers containing protected health information (PHI), or research health information (RHI) must be encrypted.

To Access a VUMC Computer

- Due to the confidential nature of information contained in a patient's medical record users are authorized access to computerized patient records only after reading, signing and agreeing to the terms in the **VUMC CONFIDENTIALITY AGREEMENT.**

- House Staff receive their **VUMC CONFIDENTIALITY AGREEMENT** through the Learning Exchange.

- Also in their welcome communications, House Staff receive information about their VUMC ID and establishing a confidential password.

To Receive Computer Assistance

House Staff can call the **Help Desk – (3-HELP or 3-4357)** 24 hours/day, 7 days/week. They may need to give the Help Desk their VUMC ID so that Help Desk staff can identify them in the system. It is acceptable for the House Staff to tell Help Desk staff their VUMC ID. Device & printer IDs may also be requested when applicable. Help Desk staff will triage the call to appropriate staff if unable to assist the House Staff.

Mobile Phone Policy for House Staff

All House Staff and other VUMC employees are required to communicate patient and other VUMC Confidential Information securely and in compliance with applicable VUMC policies*, laws, and regulatory requirements, including but not limited to those issued by The Joint Commission and Center for Medicare and Medicaid Services.

Prior to commencing training, all House Staff will be given the option of either obtaining a VUMC device or utilizing their personal device. The use of either device must be in concordance with VUMC policies. House Staff choosing to utilize a personal device should keep in mind that their phone number for that device may be made available so that the House Staff can be reached regarding patient care and/or other work-related matters, House Staff who elect to not to obtain a VUMC device but instead wish to continue to use a personal device, it is important to adhere to the following:

- They must have the designated VUMC security features installed, and
- They will be required to sign a memorandum of understanding that
    - they will use secure formats for patient care communications and
    - They will not be provided compensation for the phone, carrier service or other expenses related to their personal device.

If it is determined that the House Staff is not utilized the VUMC iPhone, then it must be returned so that the phone can be reassigned.

All mobile communications regarding patient care are expected to occur within the secure applications provided on the VUMC device. The House Staff member assigned a VUMC phone will be responsible for the proper care of the device. The VUMC phones will be serviced through the VUMC Help Desk and House Staff are required to immediately report any damage or to the VUMC Help Desk and the GME office. If it is determined that the VUMC device was damaged through improper use and lack of care in handling, or if the damage or loss is not immediately reported, the House Staff member may be required to pay a replacement cost.

Under no circumstances should personal, international long-distance calls be placed from a GME-issued iPhone.

House Staff are required to abide by all applicable VUMC policies including, but not limited to the following:

- Acceptable Use of VUMC Computing Resources Policy
- Electronic Messaging of Individually Identifiable Patient and Other VUMC Confidential or Sensitive Information
- and the corresponding SOP Approved Messaging Mechanisms
- Use of Mobile Devices to Conduct VUMC Business
- and the corresponding SOP MDM Device Requirements:

Please note that House Staff may rotate to external sites as part of their educational training (e.g., the VA Medical Center). While at these sites, they are expected to adhere to the applicable policies of those institutions, including without limitation policies related to the use of mobile devices and communication of patient information, and these policies may be different and/or more restrictive than the VUMC policies.

Long Distance Calls (V-Net)

Individual V-Net access codes may be issued to House Staff authorized to place long distance calls from a VUMC land-line phone. **Under no circumstances should personal long-distance calls be placed from a land-line phone.**

Pager Policy for House Staff

Pagers will be provided for House Staff if a pager is required.

Pagers are an important part of the current communication system within VUMC and should be maintained and monitored while on and off campus and at other off-site rotations. If a member of the House Staff is not on call or does not have the ability to have their pager with them, it should be rolled to an appropriate number for that service in order to provide the best continuity of patient care.

Repair/replacement of damaged or malfunctioning pagers is handled through American Messaging. The pager office is located inside the entrance to Medical Center North across from the coffee shop or through contact with Shelley Moore Shelley.Moore@americanmessaging.net. All pager numbers provided through GME will be maintained as GME pagers and assigned to specific training programs for re-use as new house staff join the training program. Pagers must be returned to the program coordinator/program manager or program director at the end of the GME appointment and conclusion of training.

If a pager owned by the GME office is damaged or lost, and requiring a replacement, the House Staff member may be asked to contribute towards the replacement cost.