**UNIVERSITY OF FLORIDA COLLEGE OF MEDICINE JACKSONVILLE**
**Office of Graduate Medical Education**

| POLICY: INFORMATION TECHNOLOGY | |
|---|---|
| Approved by: GMEC | Page(s): 1 of 4 |
| Approval date: 11/5/24 | Reviewed date: 05/01/07; 8/20/14; 2/28/19; 9/20/24 |
| Effective date: 06/01/05 | Revised date: 06/15/08; 1/31/11; 8/20/14; 5/20/19; 7/1/21; 10/20/22;9/20/24 |

Users of University of Florida College of Medicine-Jacksonville and Shands Jacksonville Medical Center, Inc. D/B/A UF Health Jacksonville [hospital] computing resources must comply with federal and state laws, university and hospital rules and policies, and the terms of applicable contracts including software licenses while using University computing resources. The University of Florida Acceptable Use Policy can be found at this website: https://it.ufl.edu/policies/acceptable-use/acceptable-use-policy/.

All trainees must read and acknowledge by their electronic signature that they have reviewed a copy of this policy through the evaluations module of New Innovations annually.

**Computer logon**: All trainees have been assigned a unique logon and password for all campus computers. Initial temporary Windows logon information is provided by the Office of Graduate Medical Education.

- The first time you logon, enter your Windows login name and password; you will then be prompted to change your password.
- Chose a strong password (an example of a weak password is "james1", a strong password is "j3flk23kl29")
- Do not share your chosen password with anyone. You will be responsible for any unauthorized access to any electronic systems with your password
- If you encounter a problem when logging into the system, please contact the ITS Helpdesk, at 4-7828.

**Trainees must sign off the computer after every use** to secure the workstation and prevent unauthorized access, as well as prevent subsequent activity from being recorded under their user ID. To sign off, simply press Ctrl+Alt+Del and click on the sign off option. A proper log off will end the Windows session under your user ID. If a PC is inadvertently locked under another user logon, choose the "switch user" option at the bottom left of the screen.

**E-mail accounts**: All trainees have a UF Health-Jacksonville Outlook e-mail account. All institutional and programmatic communication will be sent to this e-mail address. You may access your Outlook account from anywhere with an Internet connection by typing the address https://mail.ufandshandsjax.org (do not include www) in any internet browser. Enter the user's Windows login name and password to access the Outlook account. If the user has forgotten their password, has questions or requires additional assistance the user will contact the IT Helpdesk at (904) 244-7828.

The creation of your University of Florida Gatorlink account (used to access the myUFL online portal and UF Library services) provides the trainee with a separate @ufl.edu e-mail address. Communications regarding your Gatorlink account are sent to this e-mail address. In order to eliminate the maintenance of more than one e-mail account, all trainees should set their Gatorlink e-mail forwarding to their Jacksonville Outlook account. Do not set forwarding to any address other than your Jacksonville Outlook account as UF HIPAA standards prohibit forwarding of e-mails containing protected health information to personal or commercial accounts such as gmail.

**Internet Surf Control:** The date, time and website accessed by any user of the system are tracked by software systems in place throughout the campus. The software also has the ability to block specific websites determined by Administration to be inappropriate, as noted in UF Health Jacksonville policy I-02-019, (examples include but are not limited to: Adult/Sexually Explicit, Gambling, Hacking, Intolerance & Hate, and Personals & Dating). Streaming media, music, movies, and TV shows through the Internet are also blocked. If you access a website that has been blocked, refer to hospital policy I-02-019. If you believe you have a legitimate work-related reason to access a blocked site, please contact Human Resources at the following e-mail address HRSurfControl@jax.ufl.edu. If you have difficulty accessing any work-related seminars/conferences presented through the internet, please contact the IT Help Desk at (904) 244-7828.

| POLICY: INFORMATION TECHNOLOGY | |
|---|---|
| Approved by: GMEC | Page(s): 2 of 4 |
| Approval date: 11/5/24 | Reviewed date: 05/01/07; 8/20/14; 2/28/19; 9/20/24 |
| Effective date: 06/01/05 | Revised date: 06/15/08; 1/31/11; 8/20/14; 5/20/19; 7/1/21; 10/20/22;9/20/24 |

**Clinical Applications**: The same Windows username and password are used to access Epic. For access to other IT managed applications contact the IT Help Desk or your Program Coordinator. Users will choose a strong password and will not share that password with anyone. Individuals who choose to use their personal device to access Epic should do so using the Epic Haiku or Limerick apps.

For urgent in-patient or ambulatory Epic needs, contact the help Desk at (904) 244-7828.

**UF Evaluation System:** The University of Florida utilizes a web-based system called New Innovations™ for trainees to complete a variety of required, confidential evaluation processes throughout the academic year. Individuals will be notified by e-mail when an evaluation and/or survey has been assigned and will provide a link to the web page. Login requires the Institution name (UFJAX), a username and a password. Individual username and passwords are provided and managed by the Program Coordinator. A message will appear in the Notifications section of the Welcome Page. Click on the "complete it" link to be taken to the evaluations section of the software.

**Remote (VPN) Network Access:** All trainees have VPN access. Links to the VPN Login (Global Protect) and Epic Remote Access can be found here: http://ufhealthjax.org/employees/.

**UFCOMJ Website**: The University of Florida College of Medicine Jacksonville (UFCOMJ) and UF Health Jacksonville (hospital) collaborate to maintain a formal, cohesive identity on the Web https://med.jax.ufl.edu/. The Web pages showcase each academic department and its graduate medical education (GME) and undergraduate medical education (UGME) programs. The UFCOMJ Resident Manual is also available through the UFCOMJ GME website at https://med.jax.ufl.edu/graduate-medical-education/current-residents-fellows/.

**Technical Assistance**: If you experience any technical difficulties, please contact the ITS help desk at (904) 244-7828.

**UF Privacy and Security**

**Storage of Patient Information on Computing Devices:** UF Privacy and Security Policies place restrictions on the storage of patient information on desktop computer or other mobile computing devices. Failure to adhere to these policies may result in disciplinary actions up to and including termination of employment. Full policies can be found at https://policy.ufl.edu/topic/information-technology/

To summarize these restrictions:

1. **Securing a Desktop Computer**. Users MAY NOT save any patient information to the hard drive [C:Drive] of that computer. All patient information must be saved to a secured location on hospital's secured server. If an individual does not have a **personal directory** , call the ITS department at (904) 244-7828 and ask that they establish a **directory** for you. Individuals take appropriate measures to physically secure the desktop, including:
    a. Sign off ;
    b. Do not share the password with anyone;
    c. Lock the office;
2. **Securing a Laptop Computer**. Individuals must follow UF's Laptop Security and Data Protection protocol. Individuals MAY NOT store patient information on your laptop unless it meets each of the following requirements:

a. The laptop has had full disc encryption installed by the UF IT department or full disc encryption was pre-installed on the laptop (if lost – you will be required to provide proof of such installation);
b. Individual must also complete a Request for Authorization to place patient information on the laptop. This request may be obtained from the UF Privacy Manager @ (904) 244-6229. In addition, your Program Director must approve of the request
c. Individual agrees to notify UF IT department @ (904) 244-3672 and UF Privacy Manager (904) 244-6229 as soon as possible after the laptop is discovered to be lost or stolen;
d. If there is patient information saved to the laptop, individual will ensure that the information stored on the laptop is the minimum amount of patient information necessary (if there are files you don't need containing patient information – then delete them from your laptop);
e. Individual must protect the laptop with a strong password (see UF Security Standard TS0003). For more information on establishing a "strong" password, please refer to https://it.ufl.edu/security/learn-security/passwords/
f. Individual must protect the laptop:
   - Keep the device locked in a secure area when not in use;
   - Follow reasonable safeguards to prevent theft and/or viewing of patient health information;
   - Purchase the laptop through the UF IT Department if possible to ensure the proper encryption software is installed on the laptop.

3. Please refer to the Data Security information on the UF website https://security.ufl.edu/resources/data-security/

4. **Securing a Cell Phone/ Smartphone/ other similar portable device.** Users may store limited patient information in the **Cell Phone/ Smartphone/ other portable device** e-mails and on the calendar if the device supported by the UF Health Jacksonville IT Department that allows the device to sync with the UF Health Jacksonville Network.

   If trainee has a question about whether their device is supported on the UF Health Jacksonville Network – please call the ITS Helpdesk – at (904) 244-7828.

   If trainee uses a device that is supported by UF Health Jacksonville and actively sync'd with the Network:
   a. Trainee does not need to regularly purge calendar entries or e-mails since the information will be sync'd with the UF Health Jacksonville network;
   b. Immediately notify ITS @ 4-7828 as soon as possible after the portable device is discovered to be lost or stolen so that ITS may remotely remove the patient information on the device;
   c. Trainee must still protect the portable device with a strong password (see section 2.e. above).

   If you use a **Cell Phone/ Smartphone/ other similar portable device** that is NOT supported by UF Health Jacksonville (and is not synced with the network), then:
   a. Trainee is responsible for ensuring that the patient information stored to the device satisfies the minimum necessary requirement and the information stored on the device is the minimum amount of patient information necessary for the purpose you have chosen; this means that you must regularly purge dated and unnecessary information on your device;
   b. Trainee must also protect your device with a strong password and encrypt the information stored on the device.

| POLICY: INFORMATION TECHNOLOGY | |
|---|---|
| Approved by: GMEC | Page(s): 4 of 4 |
| Approval date: 11/5/24 | Reviewed date: 05/01/07; 8/20/14; 2/28/19; 9/20/24 |
| Effective date: 06/01/05 | Revised date: 06/15/08; 1/31/11; 8/20/14; 5/20/19; 7/1/21; 10/20/22;9/20/24 |

c. If trainee's device is lost or stolen, it is likely that we will need to contact each and every patient whose information is on the device.

To physically protect your device, you should:

a. Keep the device locked in a secure area when not in use;
b. Follow reasonable safeguards to prevent theft and/or viewing of patient health information;
c. For further guidance see the UF Privacy website http://privacy.health.ufl.edu/

5. Unacceptable Internet Use. Access to certain website types, as well as other electronic media, by trainees while on University, hospital, or affiliated equipment is strictly prohibited. Such sites/media may include, but are not limited to, those involving: adult/sexually explicit material, criminal activity, gambling, hacking, intolerance and hate, spyware, violence, and weapons. Note that legitimate need to access such material for patient care or research purposes is not subject to this ban.

**Reporting Lost Computing Devices:** If trainee loses a computing device with patient information stored on it, trainee must immediately inform the Program Director as well as the UF Privacy Manager (904) 244-6229.