UNIVERSITY OF FLORIDA COLLEGE OF MEDICINE JACKSONVILLE
Office of Educational Affairs

Original Approval Date: 06/01/04	**Subject:**	**Page 1 of 4**
Approved by: Ann Harwood-Nuss, MD; Constance K. Haan, MD, MS; Linda R. Edwards, M.D.	INFORMATION TECHNOLOGY	**Revised Date**: 06/15/08; 1/31/11; 8/20/14; 5/20/19
Original Effective Date: 06/01/05		**Reviewed Date**: 05/01/07; 8/20/14; 2/28/19

Users of University of Florida College of Medicine-Jacksonville and Shands Jacksonville Medical Center, Inc. "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/.

Computer logon: All residents have been assigned a unique logon and password for all campus computers. Initial temporary Windows logon information is provided by the Office of Educational Affairs.

- 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.

Residents and Fellows must log off the computer after every use to secure the workstation and prevent unauthorized access, as well as preventing subsequent activity from being recorded under your user ID. To log off, simply press Ctrl+Alt+Del and click on the tab "log off". DO NOT JUST HIT ENTER. This will LOCK the PC under your logon. A proper log off will end the Windows session under your user ID, but allow the PC to remain active for another user. If a PC is inadvertently locked under another resident's logon, turn the computer off and restart to reset the logon.

E-mail accounts: All residents have an Outlook Email Account. All important communication will be sent to this email address. You may access your Outlook account from anywhere with an Internet connection by typing the address https://mail.ufandshandsjax.org (do not put www) in any internet browser. Input your Windows login name and password to access your Outlook account. If you have forgotten your password, have questions or require additional assistance you may contact the IT Helpdesk at 4-7828.

The creation of your University of Florida Gatorlink account (used to access the myUFL online portal and UF Library services) provides you with a separate email address. Communications regarding your Gatorlink account are sent to this email address. In order to eliminate the maintenance of more than one email account, all Residents are required to set Gatorlink email forwarding to your 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. (See UFCOMJ myUFL and Gatorlink Account Setup Policy and Procedure for more instructions.)

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 Shands 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, you will be referred to Hospitalpolicy 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 email 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 4-7828.

Clinical Applications: Your computer username and password are used to access Epic. For access to other applications contact your Program Coordinator. Chose a strong password and do not share your chosen password with anyone.

For urgent in-patient Epic needs, contact the help Desk at 4-7828.

For urgent ambulatory Epic needs, contact 4-9300.

UF Evaluation System: The University of Florida utilizes a web based system for residents and fellows to complete a variety of required, confidential evaluation processes throughout the academic year. Access to these various evaluations is provided through the online residency management system New Innovations. Individuals will be notified by email of expected evaluation and/or survey needs. A link will be provided to the New Innovations web page. Login requires the Institution Login (UFJAX), a username and a password. Individual username and passwords are provided and managed by the Program Assistant/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: Links to the VPN and Epic can be found here: http://ufhealthjax.org/employees/. VPN is not required to access Epic remotely.

UFCOMJ Website: The University of Florida College of Medicine Jacksonville (UFCOMJ) and Hospital collaborate to maintain a formal, cohesive identity on the Web http://www.hscj.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 http://www.hscj.ufl.edu/resman.

Technical Assistance: If you experience any technical difficulties, please contact the ITS help desk at 4-7828.

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 computing devices such as desktop and laptop computers and PDAs. Your failure to adhere to these policies may result in disciplinary actions up to and including termination of employment. Full policies can be found at http://security.health.ufl.edu/policies/index.shtml, http://privacy.health.ufl.edu/policies/index.shtml

To summarize these restrictions:

1. **Securing a Desktop Computer**. If you use a desktop computer you MAY NOT save any patient information to the hard drive/C:Drive of your computer. All patient information should be saved to a secured server. If you do not have a **personal directory** on the hospital's secured server (the hospital's "H" drive), call the ITS department at 4-7828 and ask that they establish a **directory** for you on the UF server. You should also take appropriate measures to physically secure your desktop and your workstation, including:
   a. Logging off when you leave the computer;
   b. Not sharing your strong password with anyone;
   c. Locking your office when you are away from your workstation;
   d. For other suggestions on physically securing your workspace and your desktop computer see: UF Security Standards PS0005 and PS0006 http://security.health.ufl.edu/policies/index.shtml

2. **Securing a Laptop Computer**. You MAY NOT store patient information on your laptop unless you meet each of the following requirements:
   a. the laptop has had full disc encryption installed by the UFJP IS Department or full disc encryption was pre-installed on the laptop (if lost – you will be required to provide proof of such installation);
   b. You must also complete a Request for Authorization to place patient information on your laptop. This request may be obtained from the UF Privacy Manager @ 244-6229. In addition, your Program Director must approve of your placement of patient information on your laptop.
   c. If you lose your laptop or it is stolen immediately notify UFJP IS Department @ 4-3672 and UF Privacy Manager 4-6229 as soon as possible after the laptop is discovered to be lost or stolen;

d. If there is patient information saved to your laptop, you need to make sure that the information stored on your 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. You must protect the laptop with a strong Password (see UF Security Standard TS0003). This means that your password cannot be "flower" or "johnb". An example of a strong password is "flk98#&kl*". For more information on establishing a "strong" password, please refer to UF Security Standard TS0003. http://security.health.ufl.edu/

f. You must physically protect your 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 your laptop through the UFJP IS Department if possible. If you do this – then you will be assured that proper encryption software will be installed on your laptop.

3. Please refer to UF HIPAA Policy "*Security of Personal Portable Data Devices*" – which may be viewed at: http://privacy.health.ufl.edu/policies/hipaamanual/opguide/PP-OG-14-Port%20Data.pdf.

4. **Securing a Cell Phone / Smartphone / other similar portable device.** You may store limited patient information in your e-mails and calendar on your **Cell Phone / Smartphone / other portable device** – but only if you use a device supported by the UF & Shands IS Departments that allows you to sync the device with the Shands Network.

If you have a question about whether your device is supported on the Shands Network – please call the ITS Helpdesk – at 4-7828.

If you use a device that is supported by Shands and actively sync'd with the Shands Network:

a. You do not need to regularly purge your calendar entries or your e-mails since the information will be sync'd with the Shands network;

b. Immediately notify Shands ITS @ 4-7828 as soon as possible after the portable device is discovered to be lost or stolen so that Shands ITS may remotely remove the patient information on the device;

c. You must still protect the portable device with a strong Password (see UF Security Standard TS0003).

If you use a **Cell Phone / Smartphone / other similar portable device** that is NOT supported by Shands (and is not synced with the Shands network), then:

a. You are 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. You must also protect your device with a strong password and encrypt the information stored on the device.

c. If your 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 http://privacy.health.ufl.edu/policies/hipaamanual/opguide/PP-OG-13f-Port%20Data.pdf

Original Approval Date: 06/01/04	**Subject:** INFORMATION TECHNOLOGY	**Page 4 of 4**
Approved by: Ann Harwood-Nuss, MD; Constance K. Haan, MD, MS; Linda R. Edwards, M.D.		**Revised Date**: 06/15/08; 1/31/11; 8/20/14; 5/20/19
Original Effective Date: 06/01/05		**Reviewed Date**: 05/01/07; 8/20/14; 2/28/19

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 you lose a computing device with patient information stored on it, you must immediately inform your Program Director as well as the UF Privacy Manager (904) 244-6229.