

As you scroll down, you will find information in this broadcast about:

1. **Electronic Patient Record Upgrade**
2. **WOHKN (Western Ontario Health Knowledge Network)**
3. **Mental Health Forms 1 and 3**
4. **Re-application to UWO and London's hospitals**
5. **New Residents**
6. **Pagers**
7. **Discharge Planning Policy**
8. **Encryption**

#### **4.1. Electronic Patient Record Upgrade**

In preparation for the upcoming Cerner upgrade all **thin client devices** will be receiving automatic updates to the icons used for accessing the EPR, **this weekend June 16th and June 17th**. This will cause an interruption to users for approximately 5 minutes for any devices that are in use at the time. The thin client device will restart twice during this time.

**Please keep all thin clients in your area powered on to enable the update.**

The devices in the Emergency Departments and in the Operating Rooms will not be impacted by the automatic update process. The devices in these areas will be updated during the downtime scheduled for 0130h to 0930h on June 23rd.

Included in the updates will be new icons for: the Cerner AppBar, FirstNet, PowerChart and SurgiNet for the production and education domains (EDUC & LEARN). To see the new look and feel of the EPR software, click on the Learn ICON if you are using a thin client or access it from the START menu if you are using a PC.

If you are having any access issues please call the Help Desk ext 44357.

**On June 23** an upgrade to the current electronic patient record system (Cerner) will occur. This will ensure a solid foundation for moving forward with new components. To complete this upgrade planned downtime will occur at 1:30 am on Saturday June 23, 2007 until 9 am. On Saturday June 23, 2007. Please be aware of your department downtime processes and procedures. All units have a trained Super User who can help during time. It is very important for all users to set their filters before the upgrade occurs. Monitor cards on the monitors and the Super Users in your area will assist with this task.

## **2.2. WOHKN**

The Western Ontario Health Knowledge Network (WOHKN) Project includes a number of community health care partners who looked at opportunities to align with UWO and collaborate on the access of resources for physicians.

Out of this project is a change in how physicians (with the exception of LRCP and CHWO) access library resources (i.e. journals) will occur in June 2007. Physicians will access these resources electronically through the UWO library system and not from the hospital library.

Some of the changes include:

- \* A new library website to be launched in June.
- \* Full access to UWO clinical digital resources via username and password, 24/7 including remote access for all medical care, teaching and research and selected classifications in nursing teaching and research.
- \* Six LHSC based Librarians to support a client service approach
- \* Support for LonDis and drug related inquiries.

Each Professional Staff, Resident and their medical secretaries will receive notification of the change, a description of what the changes mean for them and a reminder of their UWO log in information. Notice of this change will also appear in the Professional Staff Broadcast, Resident Broadcast, and Resident Handbook.

## **3. Mental Health Forms 1 and 3**

The following process must occur to ensure the requirements and procedures for involuntary admission and detention of patients under a Form are valid:

- \* A Form 1 must be completed and signed by the attending or MRP physician
- \* At the same time a Form 1 is issued a Form 42 must be completed and presented to the patient. This form is the official notification that the MRP has informed the patient that he/she is being detained until a consultation by a psychiatrist is completed
- \* After that assessment is complete, if the patient still requires an involuntary admission, a Form 3 will be completed and signed by either the psychiatrist or by an alternate MRP that has not signed the Form 1. Normally the consulting Psychiatrist will sign this form.
- \* The Form 3 must be completed within 72 hours following the completion of a Form 1.

Information on these requirements will be included in the Resident Handbook to inform residents of the appropriate procedures.

#### **4. Re- application**

The deadline for your Re-application as a trainee at the LHSC/SJHC is now past due. If you have not already done so, please use the UWO Single Sign on to complete the steps required. All Residents must re-apply before they are granted privileges for next year. Program Directors will be notified of any Resident who has not completed their re-application requirements. Working without privileges will result in a payroll stoppage, prevent your involvement in any patient care related activities and could result in a letter of professional misconduct in your permanent file as well as reporting to the CPSO.

Access single sign on here <https://www.schulich.uwo.ca/singlesignon/>

#### **5. New Residents**

174 new PGY1 Residents will start on June 29 with New Resident Orientation to be held at 8:00am at Auditorium A at UH.

#### **5.6. Pagers**

**Pagers are the property of the hospital and are provided to their Residents through their Department. Residents have an obligation to return their pager to the department while on periods of LOA when the Resident does not have hospital/departmental duties.**

**Hospitals do not support the use of non-hospital pagers. Switchboard operators will only process pages to hospital - leased pages.**

#### **7. Discharge Planning Policy**

The new LHCS and SJHC Discharge Planning Policy was implemented June 11. This policy was developed to improve access to care by ensuring patient discharges are handled consistently in a manner that reflects our patient centered care values. The new Discharge Policy, additional information and resources are available on the hospital intranet at <http://www.lhsc.on.ca/priv/paf/>

#### **8. Encryption:**

Section 12 (1) of the *Personal Health Information Protection Act, 2004 (PHIPA)* sets out the requirement that health information custodians (LHSC and SJHC are health information custodians) must ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

The Information and Privacy Commissioner of Ontario (IPC) recognizes that the delivery of health care may require the use of PHI outside of the workplace, and that such PHI may most effectively be transported and used in electronic form.

Despite the ease of use and portability of electronic documents, it is still important that only the minimum necessary data be transported in this manner.

Because of the high risk of loss or theft of portable devices such as laptop computers, personal digital assistants (PDAs), or flash drives, staff and affiliates must ensure that PHI that is stored on portable devices is either de-identified or encrypted. It is not acceptable to rely solely on login passwords to protect PHI on devices that are easily stolen or lost. The IPC states " Passwords may prevent casual access to data on a device, but may not prevent access by knowledgeable thieves".

### **What is encryption?**

Encryption is a process by which ordinary text or data is turned into an unintelligible stream of seemingly random symbols. This process is controlled by a digital 'key,' which will allow access to the encrypted data. The key could be: something you know, such as a 'strong' password distinct from a login password, since there are well known methods for cracking login passwords; or something you have, such as a USB drive or token;

or

something about you, such as your fingerprint scan or your signature. Without the key, the data is unreadable. For example, the phrase "plain text" could be transformed to "~S\$£WÖN3@f" when encrypted. The effectiveness of encryption depends on both the encryption standard and the strength of the key used.

Encryption can be implemented in a number of different ways on mobile devices. LHSC and SJHC are considering whole disk encryption or Virtual Disk Encryption.

### **Whole disk (drive) encryption**

Sometimes referred to as whole disk encryption, this is a system in which an entire hard drive is encrypted. It is the preferred option for implementing encryption on new systems, and should be considered as a requirement for any new mobile device. Also, new system purchases may be the easiest way to implement encryption. Typically, installation on individual laptops is no more difficult than installing any other software.

Whole disk encryption is potentially the most secure option available to health information custodians who feel they must store PHI on mobile devices.

### **Virtual disk encryption**

A 'virtual' disk is a file that is created on an existing drive. The encryption software encrypts the entire file and treats it as if it were a new drive on the system. This typically requires the acquisition and installation of virtual disk or

disk imaging software. Access to the encrypted virtual drive will typically require the use of a strong password, distinct from a login password. Without the password, and the encryption software, the virtual drive is undecipherable. Virtual disks could be the only viable option on PDAs where the option of applying whole disk encryption may not be available. Virtual disks are also useful for older laptop computers. However, since many systems or software programs automatically create temporary files or backup files, virtual encryption is only effective if these unencrypted temporary or backup files are also either encrypted or deleted after use.

### **Device encryption**

An alternative to storing PHI on a laptop is to store the data on a portable storage device, such as a USB key or 'thumb drive'. Portable music players and PDAs may also have this functionality. The portability of such devices is matched by the frequency with which they are lost, which further reinforces the need for encryption.

Like hard drives, there are options to encrypt the entire device or just the parts of the device that contain PHI. If you have acquired software to create a virtual disk, as described above, this same software may well have the capability of encrypting portable storage devices.

### **Encryption standards**

Currently the standard most recommended for secure storage of data was AES, or Advanced Encryption Standard. The system LHSC and SJHC are considering is AES-256, and is considered very strong. In comparison, online banking uses 128 bit encryption.

The IPC has stated that in the event that a portable information device is lost or stolen, it will not be regarded as a privacy breach **if** sufficient safeguards were in place to ensure that PHI was not disclosed. Properly encrypted data would save organizations considerable time and money by allowing them to avoid the notification requirements of the *Act*, and prevent the potentially irreparable damage to an organization's reputation resulting from the loss or theft of PHI. More importantly, it would protect our patients and their families from the undue stress of knowing that their PHI had been lost or stolen.

The Privacy Commissioner of Ontario's Fact Sheet on Encryption of portable devices can be read in its entirety at <http://www.ipc.on.ca/index.asp?navid=46&fid1=613>

Please watch this spot for more information about implementation of encryption software at LHSC and SJHC.