Guideline on the storage of work-related electronic records

23 January 2012 – Wes Robertson, Director of IT, Faculty of Medicine

---

Electronic records created in a work context may, and very often do, contain confidential information, or personal information about one or more individuals. Due to the volume of such records created and maintained within the Faculty of Medicine, it is impracticable to clearly and consistently differentiate between such records, and other records or files which may not be so sensitive. For this reason, all work-related electronic records should be stored, secured, and accessed in compliance with FIPPA, and more specifically, in line with the General and Administrative Access and Privacy Practices of the University (posted on the Provost's website, at http://www.provost.utoronto.ca/policy.htm).

To support compliance with this guideline, the Faculty of Medicine provides a networked email (Exchange) and file server expressly intended for the storage of work-related electronic records, and specifically for confidential ones. This server is well secured, is backed up on a daily basis, is located within the Faculty itself, and is managed by IT professionals. It therefore complies with FIPPA and with the University's Access and Privacy Practices in every way, and is officially considered a "secure server environment."

With very few exceptions, work-related electronic records must be stored on and remain exclusively on the Faculty's networked email and file server, and should be accessed primarily from secure office computers, or via encrypted remote access to such computers (VPN or remote desktop). Work related electronic records should not be copied to 'shared drive' services such as DropBox or SkyDrive, as these largely US-based consumer services are not intended nor capable of providing the security or reliability or legal protections that the University is required to provide.

If work-related electronic records must be stored on such services for operational reasons, care must be taken to ensure that a) you have the authority to do so, b) they do not contain confidential or personal information, c) the sharing functionality required is not offered by the Faculty's file server, and d) it should be on a temporary basis only. Additionally, if you must take confidential electronic records out of a secure server environment, then you are required to either encrypt it or to de-identify the information; however, we strongly recommend that confidential electronic records remain in a secure server environment at all times.

On the next page is an excerpt taken from the Provost's *General and Administrative Access and Privacy Practices* document, relating to the storage and security of electronic and hard copy records. Please take the time to read the checklist, and to ensure that your records management practices adhere to it; you are also encouraged to visit the link provided, and to read the entire document (which was written with end-users in mind).

For assistance with or advice on the use of the Faculty's networked file server, secure remote access, or this guideline, please contact the Discovery Commons Service Desk at discovery.commons@utoronto.ca, or by phone at 416-978-8504.

Excerpted from *FIPPA - General and Administrative Access and Privacy Practices* (June 23, 2011). To view the entire document, visit http://www.provost.utoronto.ca/policy.htm.

Security for Personal and Other Confidential Information

Purpose and Objective

Law, policy and practice require that personal, health and other confidential information, be protected from unauthorized access.

This practice supports protection of electronic and hard copy records, consistent with law, policy and risk management practice. It does not supersede University IT security standards or measures such as those under the Chief Information Officer, but is intended to work with them.

The objective is to protect confidential information from unauthorized access, without disrupting University operations, and with measures appropriate for each type of record.

Checklist

1. Know which records in your work are confidential and require protection; e.g. records that contain personal or health information.

2. Keep hard copy confidential records in a secure institutional environment; locked in a non-public area when not in use or you are not present.

3. Keep electronic records of confidential information in a secure server environment.

4. Only take confidential records out of secure environments if you have: official authorization; operational need; and no other reasonable means to accomplish the task.

5. Only take hard copy confidential records out of a secure institutional environment, as necessary for immediate work. Protect them with strong security, including keeping records out of sight, secure lockup and other security measures offsite and at home.

6. To take confidential electronic records out of a secure server environment, encrypt your drive, memory stick or mobile device with the latest version of commercially available and supported encryption software, or de-identify the information.

7. When work permits, use depersonalized records, not personally identifiable ones.

8. Access confidential electronic records remotely using encrypted secure means such as virtual private network or encrypted remote desktop connection.

9. Encrypt attachments that contain personal or confidential information to email them to non utoronto.ca addresses. Communicate passwords by phone, not by email. Do not email or forward unencrypted personal or confidential information out of the utoronto.ca email system because it could be viewed by third parties if intercepted.