Security of Information and Confidentiality Policy
St. Joseph's Health Centre
Policy SE 10-1-1
Version 1.2
July 29, 2004

TABLE OF CONTENTS

Definition

The "Health Centre" refers to St. Joseph's Health Centre.

Commitment to Confidentiality and Authorized Release of Information

Individuals have an ethical and legal right to privacy. This right to privacy is based on respect for persons and the principle of autonomy. This ensures that the individual has control over what, and to whom, information about them is disclosed. The Health Centre recognizes its obligation to respect privacy and is committed to maintaining the confidentiality of patient, worker, and Health Centre information, whether written, verbal, electronic, photographic or stored on any other medium.

The Health Centre also has an obligation to ensure access to information by authorized individuals. Individuals also have the right to access their own personal health information as outlined in the Health Centre's Administration Manual.

What is Confidential Information?

Confidential information is information of a sensitive nature in any format which is created or received by the Health Centre in the course of its business which is not otherwise available to the public and includes, but is not limited to, the following:

- patient information — any information which could lead to the identification of a specific patient, or family member/significant other of a patient;
- financial information — any information that would outline a person's salary or any unpublished financial information (e.g., suppliers, debtors, payroll);
- human resources information — any performance-related information, compensation, benefits, WSIB, or occupational health information;
- legal information — any information outlined in a legal document (e.g., contracts, agreements, disputes);
- human rights information — any information that is associated with an informal or formal human rights complaint, including an abuse or harassment complaint;
- other administrative information — any information used for administrative purposes (e.g., schedules, patient census, employee lists, patient lists, donor lists, etc.);
- business information - any information related to the Health Centre's ongoing or strategic initiatives (e.g., organizational restructuring, mergers, outsourcing of business units).

When are you Authorized to Access Information?

As part of your association with the Health Centre, you have authority to access certain information. This access is limited, and strictly confined, to information required for performance of your current Health Centre duties. Access to patient information must be done in accordance with "Confidentiality: Use and Disclosure of Personal Health Information", Policy #: SJ-04-04-01 in the Health Centre's Administration Manual.

When can Information be Disclosed?

Disclosure of information is generally prohibited except as outlined below:

- as permitted pursuant to the Public Hospitals Act, Reg. 965, the Personal Health Information Protection Act and the Mental Health Act
- with consent (written or verbal) from the patient whose information it is.
  It is the staff's responsibility to ask all patients, or to check on the computerized patient care system under "Patient Confidentiality", if they want their basic Health Centre information (location, phone number, and condition-serious, critical, fair, etc.) given out to the public. If a patient is incapable of giving consent to the release of their information, then the information will only be released after securing consent from the patient's substitute decision maker pursuant to the Personal Health Information Protection Act
- as necessary in the performance of current Health Centre duties.
- As obliged by law when the failure to disclose information is likely to place the patient or third parties in imminent danger.
- pursuant to a Court Order, Subpoena, Summons, Search Warrant, or other legislation.
- access to one's own health record while in the Health Centre or after discharge must be done in accordance with "Confidentiality: Use and Disclosure of Personal Health Information", Policy #: SJ-04-04-01 in the Health Centre's Administration Manual
- access to an employee's record in Human Resources must be done in accordance with "Personnel Record", Policy #:SJ-08-00-35 in the Health Centre's Administration Manual.
- The Health Centre shall, through its designated Foundation or department, release information approved by a member of Senior Management for the purposes of communicating with patients and/or the fundraising of general patients. This information shall be handled in accordance with the Foundation policies and codes of ethics in the Health Centre Foundation Confidentiality of Information and Data Security document.

Even when the health care professional is obligated to disclose confidential information by law, confidentiality should be preserved to the maximum possible extent.

All inquiries from the media regardless of their nature should be immediately referred to Public and Community Affairs. After business hours, a representative from this department may be reached through Locating. Any release of information to the media must be done in accordance Media Relations policy SJ-06-04-01 in the Health Centre's Administration Manual.

All inquiries for information which are not dealt with in this section (e.g., police, lawyers, etc.) should be referred to Medical Affairs, Human Resources or the On Call Senior Management employee.

Reasonable Limits

Subject to the reasonable limits described below, confidential information must not to be discussed in any area where others not entitled to receive that information are present.
For example:

- in public areas of the Health Centre such as elevators, washrooms, lounges, stairwells, cafeteria, or shuttle buses;
- at home;
- in public places outside the Health Centre, unless required to do so by law or with permission from an authorized individual.

Confidential information should never be left in written form or displayed on computer terminals in locations where it may be seen by unauthorized persons (e.g., while transporting patients and their records through the Health Centre or leaving information on a photocopier, fax machine, or white board).

File cabinets and storage areas which contain confidential information should be kept locked when unattended.

When disposing of Confidential information it should be in accordance with "Retention and Disposition of Confidential Information", Policy #: SJ-04-04-02 in the Health Centre's Administration Manual.

What is a Breach of Confidentiality?

Breach of confidentiality includes any intentional or inadvertent unauthorized access to, or disclosure of, confidential information.

It is not a breach of confidentiality to report patient information in a Health Centre approved research study as long as the patient is not identifiable.

Consequences of Breaching Confidentiality

The Health Centre considers any breach of confidentiality, intended or unintended, as an unacceptable occurrence requiring immediate follow-up as outlined in this document.
When it is deemed that a breach of confidentiality has occurred, and there is no reasonable justification and/or explanation for the breach, the result can include disciplinary action up to and including immediate dismissal and/or loss of all Health Centre privileges.

Examples of breach of confidentiality:

- obtaining unauthorized access to family member's patient recoreds
- unauthorized access to one's own patient records
- allowing another person unauthorized access to patients records
- discussing any individual's personal or confidential information when such discussion is not authorized as necessary to your role
- unauthorized access to an employee's confidential personnel or payroll information

Confidentiality Audits

Audits will be conducted periodically on records of a confidential nature to monitor compliance with Health Centre policy.

Data Security

All Health Centre computer systems and much of the data residing on them are vital corporate assets. Individuals are responsible for protecting corporate data and patient information entrusted to them.

Access to all corporate data must be properly authorized and will be granted based on the requirements for carrying out Health Centre responsibilities and duties. The Health Centre retains the exclusive rights to, and use of, all computer assets and information which it owns and safeguards, and which reside on:

- Health Centre mainframe processing systems;
- Health Centre systems residing on local area networks, enterprise networks, and/or standalone microcomputers or any other devices;
- The Health Centre voice mail and e-mail systems.

To have authorized access to a system, a user requires a sign-on. A sign-on consists of a login ID and password and is the prerequisite to the use of an individual's electronic signature. An electronic signature establishes authorship and validity of a statement, order, document, report, or record by an electronic means.

A user is prohibited from:

- using another person’s account
- disclosing any passwords to another individual
- attempting to, or gaining access to any data to which they are not authorized

When it is deemed that a user has violated this section of the policy the Director of Information Services will contact the individual's supervisor to inform them of the breach of security. The supervisor will be asked to review the policy with the individual and ensure that the policy is followed. Subsequent failure to abide by this policy can result in disciplinary actions up to and including disabling user access to the system and dismissal from the Health Centre and/or loss of privileges.

Users should not leave a workstation unattended while a session is in progress, with the exception of computers in a restricted area (as defined by Information Services) where workers are performing a similar function. To secure confidential information, users must password protect files and log-off when leaving a workstation unattended.

All entries into confidential records must be dated and authenticated. Such authentication may include written or electronic signature.

Review of Policy and Signing of the Confidentiality and Security Agreement

1. At the time of orientation, this confidentiality and security policy will be reviewed with new Health Centre employees, members of the medical staff, researchers, contracted professionals and non-professionals, students, volunteers, and any other individual working at the Health Centre. Each individual will be required to sign the Confidentiality and Security Usage Agreement Form SE10-1-2 prior to receiving a Health Centre identification badge

2. All existing Health Centre employees, members of the medical staff, researchers, contracted professionals and non-professionals, students, volunteers, and any other individual working at the Health Centre will also be required to review and sign the Confidentiality and Security Agreement Form SE10-1-2

3. The signed copy of the Agreement will be placed on the employee's personnel record. Signed copies of the Agreement for Volunteers, Medical Staff and Students will be retained on the respective department files.

Systems Access

In order for Health Centre employees, members of the medical staff, researchers, contracted professionals and non-professionals, students, volunteers, and any other individual working at the Health Centre to gain authorized access the following steps must be completed

1. The manager, director or appropriate staff supervisor shall complete a **Request for new USER account** Form 10-1-1 and forward it to Information Services Help Desk.

2. Information Services will confirm whether the request for system access is appropriate and properly authorized and, if so, will create a user account with the level of security necessary and contact the user to inform them that the request has been processed.

3. The User will then present themselves to the Information Services department along with valid identification and only then will users receive their passwords.

4. Persons who require new passwords shall advise their manager who shall contact Information Services Help Desk.

Storage/Handling of Electronic Information

Confidential documents (e.g. correspondence, spreadsheets) should be stored on the user's personal folder (h: drive) not on the PC's hard drive (i.e. c: or d:)

Users should be aware that information stored on shared drives (e.g. n: q:) can be accessed by others who have rights to that folder.

Information stored on Laptop computers and floppy diskettes are prone to becoming a source of confidentiality breaches. All reasonable precautions should be undertaken to ensure that breaches do not occur.

Voice-Mail

Always exercise a degree of caution when using the Health Centre's voice messaging system. When leaving messages or forwarding messages be sure that messages are not inadvertently sent to incorrect

voice mailboxes. In particular, exercise particular care when using Phone distribution Lists. Refrain from forwarding messages containing SJHC confidential information to multiple parties unless there is a clear business need to do so. Be aware that sent Voice Messages cannot be deleted from a recipients mailbox.

E-Mail

Employees must also exercise a greater degree of caution in transmitting SJHC confidential information via the E-mail system than they take with other means of communicating information. Confidential Health Centre information should never be transmitted or forwarded to outside individuals or companies not authorized to receive that information or be sent or forwarded to other employees within SJHC who do not need to know the information. Always use care in addressing E-mail messages to make sure that messages are not inadvertently sent to outsiders or the wrong person inside the Hospital. Again, be particularly careful when using distribution lists ensuring that all addressees are appropriate recipients of the information. Note that once sent, messages cannot be deleted or "unsent" by the e-mail administrators.

Internet E-mail and the Internet

Internet E-mail and the Internet in general are not secure and should not be used to send or receive confidential information unless encryption is used during the information exchange. Correspondents wanting to send you (or asking that you send them) non-encrypted confidential information via the Internet must be discouraged from doing so.

Internet Usage

The Health Centre recognizes the need for provision of access to the Internet as a means to communicate with peers and access on-line resources, with the specific objective to enhance patient care or hospital practices. It is a business interest of the Health Centre that the internet not be used for reasons other than those that directly contribute to the business operations and the services to its customers. The procedures of this policy provide guidance and direction to all employees/physicians /volunteers regarding the use of the Internet.

I. Appropriate Uses of the Internet and Limitations:

Internet access/usage are appropriate when they either directly or indirectly support the provision of services or the business practices necessary for the operation of St. Joseph's Health Centre. Usage of the Internet for browsing/communications of a personal nature is generally considered inappropriate as described in procedure II of this policy.

II. Inappropriate Uses of the Internet:

Internet access/usage are inappropriate when they do not support the care processes or business practice of the Health Centre. It is understood that it is possible to access questionable material, and material unsuitable for Health Centre use on the Internet. It is also understood that the individual has sole control over what he/she is accessing. If it is found that the individual has or is accessing inappropriate web-sites/material, the individual will be reported immediately to Health Centre Administration.

Downloading of files and programs (i.e. screen savers, wallpaper images, music, etc.) from the Internet is strictly prohibited.

(Please refer to SJHC Internet Access and Usage Policy 10.2.1 for further detail)

FAX

Before using FAX machines to transmit confidential information, SJHC staff must ensure that recipients have agreed to receive confidential information in this manner and that they have confirmed that their FAX equipment is secure. A FAX cover page that clearly identifies the intended recipient should always be used and a disclaimer must be placed on that FAX cover page, for example:

> This fax is directed in confidence solely to the person named above, and may not be otherwise distributed. If you have received this telecopy in error, please notify us immediately by telephone and return the original transmission to us by mail, or destroy the same, without making a copy. Thank you for your assistance.

FAX machines used to receive confidential information must be located in physically secure areas or attended by authorized personnel. Confidential FAX documents received must be promptly forwarded to the intended recipient. FAX documents intended for the Hospital but sent to the wrong number should be forwarded to the intended recipient, if identifiable, and the sender notified of the error.

Documentation of Inadvertent Access into Confidential Patient Information

1. If anyone inadvertently accesses Confidential Patient Information to which they are not authorized, that individual must immediately complete a "Record of Inadvertent Access into Confidential Patient Information Record" Form 10-1-3 and submit this documentation to his/her supervisor.

2. Documentation of inadvertent access must include the following information:

    - date of access;
    - the patient's ID (MRN);
    - reason for access;
    - source of access
    - Individual’s name, position, and unit area.

The supervisor must then forward this form to the Director of Information Services. The information on this form will be used to verify inadvertent access as part of the confidentiality audit process.

Confidentiality Audits for Patient Electronic Records

The Director of Information Services or his/her designate will conduct confidentiality audits on patient electronic records. An arbitrary time frame within each Bi-monthly period will be identified for the audit. Patient records are selected and reviewed to identify those individuals who have accessed the record without also having written to the record.

Results from the audit are sent to the Vice President or his/her designate responsible for the individual identified in the audit. The Vice President or his/her designate reviews the information with the person to whom that individual reports. If, in consultation with the individual named in the audit, it is established that the individual had no authority to access the record, or if authority to access is in question, then the matter is referred to Senior Management.

Senior Management meets with the named individual (and union or other representative, if applicable) to assess the situation and to determine whether there was reasonable justification for the breach, and then makes recommendations regarding consequences. Where the individual is a member of the medical staff, a recommendation regarding consequences is also made to the Chairman of the Medical Advisory Committee.

With respect to patient-initiated requests any patients who believe that their records have been inappropriately accessed must submit a written request for an audit to the Director, Information Services. Requests of this nature will be accommodated where practical and a letter of follow-up will be sent to the patient that requested the audit.

Reporting a Breach of Confidentiality

Every person working at the Health Centre has the right and responsibility to report a breach of confidentiality without fear of reprisal for doing so.

If an intentional or inadvertent breach of confidentiality is suspected to have occurred, the following steps must be taken to report the incident:

The witness must submit in writing a description of the incident in writing to the Director of Information Services. The description should outline:

- when (dates and times), where, and how the suspected breach occurred;
- who was involved in committing the suspected breach;
- names of other people who witnessed the suspected breach.

The Director of Information Services or his/her designate will acknowledge receipt of the incident report by sending a written confirmation to the witness.

The Director of Information Services or his/her designate will send the incident report to the Vice President or his/her designate that is accountable for the individual suspected to have breached confidentiality. The incident report is then reviewed with the named individual to determine its accuracy. If further investigation is warranted, then the matter is referred to Senior Management. Senior Management meets with the named individual (and union or other representative, if applicable) to further assess the situation and to determine whether there was reasonable justification for the breach, and then makes recommendations regarding consequences. Where the individual is a member of the Medical Staff, a recommendation regarding consequences is also made to the Chairman of the Medical Advisory Committee.

Changes to Employee Status

Managers are required to promptly inform Human Resources of all employee transfers, terminations, leaves of absence, or maternity leaves. Human Resources must also notify the Information Services Help Desk of any changes to an employee's status so that user accounts can be modified or deactivated as required.

ST. JOSEPH'S HEALTH CENTRE

ADMINISTRATIVE POLICY & PROCEDURE MANUAL

Record of Inadvertent Access into a Patient's Confidential Information - Form SE10-1-3

Date: (mm/dd/yyyy)____/____/_____

Name & Position: (please print)_____

Unit/Department: _____

Date of inadvertent access: (mm/dd/yyyy)____/___/____

Source of access:_____

Actual time of access:____:_____

J # of Patient's chart entered (if known) :_____

Name of Patient's chart entered (if known) :_____

Comments:
_____
_____
_____
_____
_____

Signature: _____

Signature of supervisor/manager: _____

The supervisor must forward this record to Director of Information Services. Information Services will acknowledge receipt of this record.

FOR DIRECTOR OF INFORMATION SERVICESS USE ONLY
Date received: (mm/dd/yyyy) ___/___/____
Data Security personnel signature: _____

ST. JOSEPH'S HEALTH CENTRE

Confidentiality and Security Agreement - Form SE10-1-2

This agreement extends to all employees, medical staff, volunteers, students, outside consultants, contract personnel and office personnel of physicians with remote access.

It is the policy of ST. JOSEPH'S HEALTH CENTRE to maintain the confidentiality of all patient and employee information and certain business information. The hospital has a legal and ethical responsibility to safeguard the privacy of all patients. The hospital also has the responsibility to secure and protect the confidentiality of all patient and employee information.

In the course of and following my employment/assignment/appointment within ST. JOSEPH'S HEALTH CENTRE, I will hold all information confidential whether health related, personal, social and /or psychological concerning patients, staff and any other person having an affiliation with ST. JOSEPH'S HEALTH CENTRE. I agree that I will not access information on patients for whom I do not have responsibilities, nor access patient or other information unless access to pertinent information is required to perform duties related to my position. I understand that such information must be maintained in the strictest confidence at all times including the workplace and outside. As a condition of my employment/assignment/appointment, I agree to follow ST. JOSEPH'S HEALTH CENTRE's "Security of Information and Confidentiality" (Policy #: SE 10-1-1) and "Internet Access and Usage" (Policy #: 10-1-2) policies, and Information Services best practices at all times while I am associated with the hospital and after my association ends. I understand that sharing any information except in the direct performance of duties related to my position is a violation of trust placed in me by the organization.

I understand that as a user of the ST. JOSEPH'S HEALTH CENTRE Information Systems, my user identification code and password is considered the equivalent of my signature. I am responsible for all transactions performed using this code and/or passwords and agree not to disclose the same to anyone or to attempt to acquire or use another person's code or password. If I have reason to believe that my identification code is known, lost or stolen, I will immediately act to have my password changed.

I understand that any violation of this agreement may result in the loss of computer system access, legal, and/or other corrective action up to and including termination of my employment/loss of privileges.

_____	_____
Signature	Witness Signature
_____	_____
Print Name	Witness – Print Name
_____	_____
Position	Date
_____	
Department	