ADMINISTRATION MANUAL

TITLE: Security of Information and Confidentiality **POLICY #:SJ10-01-01**

SECTION: Information Services

ISSUING AUTHORITY: Senior Leadership Team, Medical Advisory Committee

ORIGINAL DATE APPROVED: July 29, 2004,
SUBSEQUENT APPROVAL DATES: September 2015

POLICY:
This policy applies to: physicians, other medical staff, employees, volunteers, students, researchers, third-party service providers, and any other agent associated with St. Joseph's Health Centre (Health Centre). This policy relates to the use of E-mail, voice-mail, laptops, removable media or mobile devices to provide health care or to the Health Centre's business operations, and information in written, verbal, electronic, photographic or stored on any other medium, including accessing information on the Internet at SJHC and when logging in remotely.

The Health Centre recognizes its obligation to respect privacy, security and confidentiality of personal, patient, and confidential information. At the same time the Health Centre recognizes its obligation to ensure access to information by authorized individuals. (See Appendix C)

It also holds users accountable for their actions and requires them to sign the attached Confidentiality and Security Agreement (Form SE10-1-2, see Appendix A). Individuals are responsible for protecting corporate data and personal health information (PHI) and personal information (PI) under their custody or control.

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 servers and storage devices
- Health Centre systems residing on SJHC networks, and/or standalone computers or any other devices;
- The Health Centre voice mail and e-mail systems.

Violations of this policy by physicians, other medical staff, employees, volunteers, students, researchers, third-party service providers, and any other agent associated with the Health Centre may result in loss of privileges, or corrective or disciplinary actions up to and including

written warnings, suspensions and dismissal, being taken. Violations of this policy by contractors or consultants of the Health Centre may result in cancellation of contracts and/or loss of privileges. Violations of this policy may result in application of the Workplace Harassment and Discrimination Policy or in the case of physicians a referral to the Chief of Staff for appropriate action.

Disclosure of Information

Disclosure of information is generally prohibited except as outlined below:

- it is the staff's responsibility to ask all patients/substitute-decision maker, if general basic information (e.g., presence, health status) can be shared at the public's request.
- as permitted pursuant to the Public Hospitals Act, Reg. 965, the Personal Health Information Protection Act, Mental Health Act, Freedom of Information and Protection of Privacy Act (FIPPA)
- 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
- in accordance with PHIPA the Health Centre shall release to its designated Foundation the names and contact information, unless the patient has given express instruction not to disclose.

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 *Corporate Communications and Public Affairs, Media Relations Policy #SJ06-04-01*.

All inquiries for information which are not dealt with in this section (e.g., police, lawyers, etc.) should be referred as appropriate to Manager, Quality Strategic Information and Performance Systems, Medical Affairs, Human Resources or the On Call Senior Leadership employee.

Confidential information must not to be discussed in any area where others not entitled to receive that information are present.

Disposing of Confidential Information

When disposing of confidential information it should be in accordance with *Retention and Disposition of Patient Health Records Policy # SJ-04-04-02* and *Retention of Hospital Records Policy #SJ 02-02-05*.

Storage/Handling of Electronic Information

Confidential documents (e.g. correspondence, spreadsheets) should be stored on the user's personal folder (h: drive) and/or other shared network drives not on the PC's local storage (e.g., c:).

PI and PHI stored on laptop computers, mobile devices, and removal media have a higher risk of loss or theft resulting breaches of confidentiality. All reasonable precautions should be undertaken to ensure that breaches to one or more individuals do not occur. This means the file, the device, or removable media must be encrypted. All SJHC portable devices must be encrypted, e.g. laptops. Users requiring USB storage media containing PI and PHI must obtain an encrypted device through Information Services.

Confidentiality Audits

The Information Access and Privacy Office (IAPO) conduct periodic confidentiality audits on patient electronic and paper records to monitor compliance. (See Appendix C)

The Health Centre will conduct audits of patient records and information systems as required.

Breach of Confidentiality

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

Examples of breach of confidentiality:
- 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

Documentation of Inadvertent Access into Confidential Information

Any inadvertent access to confidential information where an individual does not have authorization to do so, is considered as a breach of confidentiality and it must be reported to your immediate supervisor and the Record of Inadvertent Access into a Patient's Confidential Information form (see Appendix B) is completed and forwarded to the IAPO.

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. All breaches of confidentiality should be reported to your immediate supervisor and the IAPO. (See Appendix C)

SJHC will contact shared systems when breaches of privacy are found in one or more shared systems.

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 policy. 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. (See Appendix C)

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 notifies the Information Services Help Desk of any changes to an employee's status so that user accounts can be modified or deactivated as required.

DATA SECURITY:

Users should not leave a workstation in an open-area unattended while a session is in progress, to secure confidential information, users must log-off when leaving a workstation.

Voice-Mail

Always exercise 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 Health Centre confidential information to multiple parties unless there is a clear business need to do so. Be aware that forwarded Voice Messages cannot be deleted from a recipient's mailbox by the sender.

Health Centre's E-Mail System

Employees must also exercise caution in transmitting the Health Centre's confidential information via the internal E-mail system (e.g. GroupWise). See E-mail Usage Policy SJHC-TBD.

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 may contain privileged information which is only intended for the recipient(s). If you are not the intended recipient, please inform the sender at 416-530-6000 and destroy this fax plus any attachment(s) associated with it.

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.

Internet Usage

See the Computer and Internet Acceptable Use Policy # SJ 10-02-01.

Conversations

When possible, discussing confidential information in the following areas should be avoided:
• in public areas of the Health Centre
• at home
• in public places outside the Health Centre, unless required to do so by law or with the permission from an authorized individual.

Protecting Documentation

•Confidential information should never be left in written or printed form 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.
•Open filing cabinets should have a barrier between it and the public (e.g., cabinet placed behind a counter)
•Computer terminals should face away from passers-by

DEFINITIONS:

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;

Personal Information (**PI**) – recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

Examples:
- 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).

Personal Health Information (PHI)

- Information about an individual whether living or deceased and whether in oral or recorded form. It is information that can identify an individual and that relates to matters such as the individual's physical or mental health, the provision of health care to the individual, payments or eligibility for health care in respect of the individual, the donation by the individual of a body part or bodily substance, and the individuals health number. (PHIPA 2004)

- Personal health information can be information about a physician or other care provider, a staff person, a patient, or a patient's family member. Examples of personal health information include a name, medical record number, health insurance number, address, telephone number, and personal health information related to a patient's care such as blood type, x-rays, consultation notes, etc.

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

Removable Media means a storage device that can be removed from a computer, such as a CD ROM, hard disk, and usb drive.

Substitute-Decision Maker in relation to a individual, means, unless the context requires otherwise, a person who is authorized under PHIPA to consent on behalf of the individual to the collection, use or disclosure of patient information about the individual

Third-Party Service Providers – for the purpose of this policy it refers to anyone that the Health Centre has a contract for services.

REFERENCES:

CROSS REFERENCE:

Personnel Record Policy #SJ-08-00-35
Computer and Internet Acceptable Use Policy #: SJ-10-02-01
Personal Health Information and Vulnerable Digital Devices Policy, # TBD

REGULATORY REFERENCE:

Freedom of Information and Protection of Privacy Act (FIPPA)
FIPPA, Regulation R.R.O. 1990, REGULATION 460
Public Hospitals Act, Reg. 965
The Personal Health Information Protection Act (PHIPA)
PHIPA, ONTARIO REGULATION 329/04
Mental Health Act

DEVELOPED BY: Information Services (IS), Information Access and Privacy Office (IAPO)

REVIEWED BY: IS, IAPO, Health Records, Human Resources, Medical Affairs, Enterprise Risk Management, Corporate Communications and Public Affairs, Patient Relations

DISTRIBUTION: Everyone

FORMS

Form SE10-1-3: Record of Inadvertent Access into a Patient's Confidential Information - Form
Form SE10-1-2: The St. Joseph's Health Centre Confidentiality and Security Agreement

APPENDIX A
ST. JOSEPH'S HEALTH CENTRE
Confidentiality and Security Agreement - Form SE10-1-2

This agreement extends to all employees, physicians, other medical staff, volunteers, students, researchers, consultants, third-party service providers and any other individual affiliated with ST. JOSEPH'S HEALTH CENTRE. It applies to the rules of conduct concerning confidential personal, medical and patient information through on site and 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 personal 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 # SJ-10-01-01), Computer and Internet Acceptable Use Policy" (Policy # SJ-10-02-01) and Personal Health Information and Vulnerable Digital Devices (Policy #TBD policies, and Information Services and the Information Access and Privacy Office 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.

Violations of this policy by physicians, other medical staff, employees, volunteers, students, researchers, third-party service providers, and any other agent associated with the Health Centre may result in loss of privileges, or corrective or disciplinary actions up to and including written warnings, suspensions and dismissal, being taken. Violations of this policy by contractors or consultants of the Health Centre may result in cancellation of contracts and/or loss of privileges. Violations of this policy may result in application of the Workplace Harassment and Discrimination Policy or in the case of physicians a referral to the Chief of Staff for appropriate action.

I acknowledge that I understand and agree to comply with the Security of Information and Confidentiality Policy # SJ10-01-01.

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

APPENDIX B

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 the Information Access and Privacy Office (IAPO) who will acknowledge receipt of this record.

FOR IAPO USE ONLY
Date received: (mm/dd/yyyy) ___/___/____
Data Security personnel signature: _____

APPENDIX C

Security of Information and Confidentiality Procedure

Description:
This procedure covers the steps to follow to protect the privacy, security and confidentiality of personal, patient and confidential information.

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 computer systems access, the following steps must be completed

1. The manager, director or appropriate staff supervisor shall complete and submit a **Help Desk Request Form** found on SJNet which is automatically forwarded 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 new staff member must have a valid identification with a picture in order to receive their new account credentials.

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

Confidentiality Audits

The IAPO runs regular access audits on Sunrise Clinical Manager. If someone is suspected of a breach, the IAPO will notify his/her manager. The manager will discuss with the employee if it was an inappropriate access. If a privacy breach has occurred the matter will be escalated to Human Resources which can result in loss of privileges, or corrective or disciplinary actions up to and including written warnings, suspensions and dismissal, being taken.

Documentation of Inadvertent Access into Confidential Information

1. If a staff member inadvertently accesses confidential patient information to which they are not authorized, that individual must immediately complete a "Record of Inadvertent Access into Patient's Confidential Information Record" Form 10-1-3 (see Appendix B)and submit this documentation to his/her supervisor.

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

Reporting a Breach of Confidentiality

If an intentional or inadvertent breach of confidentiality is suspected to have occurred, the witness should report this to the IAPO.

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

Violations of Policy

Violations of this policy by physicians, other medical staff, employees, volunteers, students, researchers, third-party service providers, and any other agent associated with the Health Centre may result in loss of privileges, or corrective or disciplinary actions up to and including written warnings, suspensions and dismissal, being taken. Violations of this policy by contractors or consultants of the Health Centre may result in cancellation of contracts and/or loss of privileges. Violations of this policy may result in application of the Workplace Harassment and Discrimination Policy or in the case of physicians a referral to the Chief of Staff for appropriate action.