St. Joseph's Healthcare Hamilton	MANUAL CORPORATE	Section ADMIN	Pages 8	Number 090-ADM
Subject: PRIVACY OF PERSONAL INFORMATION			Date March 25, 2015	
Supersedes: February, 2015	Cross Reference: 045-ADM, 060-ADM, 092-ADM, 012-HIS, 069-MED		Issuing Authority: PRIVACY OFFICE	
☑ Charlton Campus	☑ West 5th Campus		☑ King Campus	

Table of Contents

1.0 Purpose & Goals Description

To establish guidelines for the collection, use and disclosure of personal health information, to protect the rights and privacy of patients and clients of SJHH while supporting safe, quality care and services in compliance with the *Personal Health Information Protection Act (PHIPA), 2004*.

2.0 Definitions

AGENT in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated.[1]

CIRCLE OF CARE is a concept that allows for the exchange of personal health information between and among healthcare providers that are involved in providing healthcare services to a patient without express patient consent.

CONFIDENTIALITY refers to the obligation upon an organization or person to protect information that has been entrusted in its care for a specific purpose, and to ensure that information is only accessible to those authorized to have access and is used only for the purpose for which it was

obtained and for no other purpose. Thus, confidentiality refers to organizational or professional duties, whereas privacy refers to individual rights to their information at large.[3]

CONSENT means the informed voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.[2] In either case, consent must be given without deception or coercion.

DISCLOSURE in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian or to another person, but does not include to use the information, and "disclosure" has a corresponding meaning.[1]

LEGAL REPRESENTATIVE /SUBSTITUTE DECISION MAKER (SDM) means a person who has legal authority to make decisions on behalf of another person.

PERSONAL INFORMATION includes any factual or subjective information, recorded or not, about an identifiable individual (for example, age, name, ID numbers, income, ethnic origin, social status). *Personal information does not include the name, title, and business address or business telephone number of an employee of an organization.*

Personal Information includes **PERSONAL HEALTH INFORMATION (PHI)**, means identifying information about an individual in oral or recorded form, if the information,

a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,

b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,

c) is a plan of service within the meaning of the *Long-Term Care Act, 1994* for the individual,

d) relates to payments or eligibility for health care in respect of the individual,

e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,

f) is the individual's health number, or

g) identifies an individual's substitute decision-maker [1]

PRIVACY refers to the right of an individual to control who has access to his or her personal information and under what circumstances.[4]

RECORD means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record.[1]

SECURITY is characterized as the preservation of the confidentiality, integrity and availability of personal information. Information security is achieved by or through physical, organizational and technical means, including implementing policies and procedures based on relevant legislation, standards and ethical principles, careful planning, design, implementation and maintenance of

appropriate technology solutions and managing ongoing operations related to the collection, classification, access and disclosure of personal information.[4]

USE in relation to personal health information in the custody or under the control of a health information custodian or a person, means to handle or deal with the information, subject to subsection 6 (1), but does not include to disclose the information, and "use", as a noun, has a corresponding meaning.[1]

3.0 Equipment/Supplies

None

4.0 Policy

All personal information under the care, custody and control of SJHH shall be regarded as confidential and available only to authorized users. Subject to specific legislative limitations and exceptions, patients/clients (or their legal representatives) may access their own personal information contained in records held by SJHH.

5.0 Procedure

PHIPA is structured on the 10 Fair Information Practices principles published by the Canadian Standards Association (CSA), which form the basis of most privacy legislation around the world.

Principle 1 – Accountability for Personal Information

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Accountability for SJHH's compliance with the principles rests with the Board and/or CEO having overall accountability, with delegated authority to the Chief Privacy Officer, (CPO) although other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

The Chief Privacy Officer shall oversee SJHH's compliance with the principles.

SJHH shall be responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. SJHH shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

SJHH shall develop and implement policies and practices to give effect to this principle.

Principle 2 – Identifying Purposes for Collecting Personal Information

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

The primary purposes for which personal information is collected are: the provision/delivery of healthcare, patient health education, teaching of medical and other health care students, quality assurance/risk management activities, research and statistical analysis, fundraising, and to meet legal and regulatory requirements.

SJHH shall identify the purposes for which personal information is collected in order to comply with this Principle, the Openness Principle (#8) and the Individual Access Principle (#9).

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required or permitted by law, the consent of the individual is required before information can be used for that purpose.

Persons who collect personal information will be able to explain the purpose(s) for which the information is being collected. An admission or appointment form, brochures and/or signage may give notice of the purposes for which personal information is being collected (see Principle #8).

Principle 3 – Consent for Collection, Use and Disclosure of Personal Information

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Where possible and practicable, SJHH shall seek consent for the use or disclosure of personal information at the time of collection.

SJHH shall make a reasonable effort to ensure that individuals are advised of the purposes for which the information will be used or disclosed. To make the consent meaningful (i.e. knowledgeable), the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

In determining the form of consent sought to collect, use or disclose personal information (implied/express, verbal/written), SJHH shall take into account the sensitivity of the information, for example, any reference to sexual/physical abuse, HIV/AIDS, communicable diseases, and mental health concerns and shall also consider the circumstances and the practicality of obtaining express consent.

In obtaining consent, the reasonable expectations of the individual are relevant. For example, an individual coming to SJHH for tests will reasonably expect that SJHH, in addition to using the individual's personal information for treatment purposes, will also contact the referring physician to report results or place the individual on a waiting list. In some cases, SJHH may assume the individual's request for service constitutes an implied consent for specific, related purposes. In contrast, an individual would not reasonably expect that personal information given to SJHH would be given to a company selling health care products, for example, unless explicit consent was obtained. In certain circumstances personal information may be collected, used, or disclosed without the consent of the individual. For example, legal or security reasons may make it impracticable to seek consent. When personal information is disclosed for the detection and prevention of fraud or for law enforcement purposes, seeking the consent of the individual may defeat the purpose of collecting the information.

SJHH's Consent to Treatment (060-ADM) Policy will apply to emergency situations, incapable patients and substitute decision-makers, in so far as informed consent is required.

The way in which SJHH seeks consent may vary, depending on the circumstances, the type of information collected and the requirements of applicable legislation. An authorized representative such as a legal guardian, substitute decision-maker as defined under the *Health Care Consent Act, 1996*, or patient's representative under the *Mental Health Act* may consent to the collection, use or disclosure of personal information on behalf of the person whom they are legally authorized to represent.

Individuals may give consent in many ways—for example:

- An admission or appointment form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
- Consent may be given orally when information is collected over the telephone, and should be so recorded; or
- Consent may be given at the time that the individual receives a service or treatment.
- Consent shall not be obtained through deception or coercion.

Consent may be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice. SJHH shall inform the individual of the right to and the implications of withdrawal of consent. Withdrawal is not retrospective and is only valid on a 'day forward' basis.

Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

SJHH shall specify the type of information that may be collected as part of its information-management policies and practices, in accordance with the Openness principle. Both the amount and type of personal information collected will be limited to that which is necessary to fulfill the purposes identified.

Principle 5 – Limiting Use, Disclosure, and Retention of Personal Information

Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information will be retained only as long as necessary for the fulfillment of those purposes.

When using personal information for a new purpose, SJHH will document this purpose.

SJHH and individual departments, as appropriate, shall develop policies, guidelines and/or procedures with respect to the disclosure and retention of personal information. Legislative requirements with respect to the retention and destruction of personal information will be applicable.

Patient health records created by SJHH will be maintained such that previous records will be pulled forward and filed with current activity records. Records will be stored in hard copy until they are eligible for destruction. See 069-MED

Principle 6 – Accuracy of Personal Information

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

The extent to which personal information will be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information will be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual. Organizational, professional, legislative and industry standards will be taken into consideration, as applicable.

SJHH will update personal information, to ensure that it is accurate and complete This is performed at each registration.

Principle 7 – Safeguards for Personal Information

Security safeguards appropriate to the sensitivity of the information shall protect personal information.

The Security safeguards will protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. SJHH will protect personal information regardless of the format in which it is held. Each department will routinely review and update its policies and procedures to safeguard personal information, specific to its circumstances.

The methods of protection will include the following measures:

- Physical (e.g. whiteboards will include only first name and last initial, locked filing cabinets, etc.)
- Organizational (e.g. confidentiality agreements and limited access for staff)
- Technological (e.g. the use of passwords, access controls)

SJHH will make its employees and agents aware of the importance of maintaining the confidentiality and privacy of personal information through education, awareness campaigns and the use of confidentiality agreements.

Care will be used in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information.

Principle 8 – Openness about Privacy Policy

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

SJHH shall be open about its policies and practices with respect to the management of personal information. Individuals will be able to acquire information about its policies and practices without unreasonable effort. This information will be made available in a form that is generally understandable.

Information made available will include:

- The name or title and address of the person who is accountable for SJHH's policies and practices, and to whom complaints or inquiries can be forwarded;
- The means of gaining access to personal information held by SJHH;
- A description of the types of personal information held by SJHH, including a general account of its use;
- A copy of any brochures or other information that explain SJHH's policies, standards or codes; and
- What personal information is made available to related organizations (e.g. the Foundation).

SJHH makes information on its policies and practices available in a variety of ways. For example, brochures are available in high-traffic patient areas (e.g. the emergency room), hospital information practices are posted in public areas, information is published online, and an informational telephone number is published on SJHH Internet page.

Principle 9 – Individual Access to Personal Information

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and will be given access to that information. An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Upon request, SJHH will inform an individual whether or not it holds personal information about the individual. SJHH will allow the individual access to this information in accordance with applicable legislative requirements. In order to receive access to one's own hospital record, a written request must be made to SJHH's Health Records Department. In compliance with PHIPA and the Mental Health Act (MHA), SJHH has processes in place relating to access and disclosure of mental health records.

An individual is required to provide sufficient information so as to permit SJHH to provide an account of the existence, use, and disclosure of his or her personal information. The information provided will only be used for this purpose. SJHH may choose to make sensitive medical information available through a medical practitioner.

When an individual demonstrates the inaccuracy or incompleteness of personal information to the satisfaction of SJHH, and depending upon the nature of the information challenged, an amendment may be made involving the correction, or addition of information that will be included as an addendum to the health record, in accordance with professional and organizational standards. Clinical information and opinions will not be deleted from the health record.

In certain situations, SJHH may not be able to provide access to all personal information about an individual. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed due to legal, security or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

Principle 10 – Challenging Compliance with the Privacy Policy

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

The CEO or Chief Privacy Officer shall be accountable for SJHH's compliance with these Principles and legislative requirements under PHIPA. SJHH will put procedures in place to receive and respond to complaints or inquiries about policies and practices relating to the handling of personal information. SJHH is committed to investigating all complaints and to taking appropriate action, including where necessary, amending policies and practices.

6.0 Documentation

None

7.0 References

- Ontario, Provincial Legislature, Personal Health Information Protection Act, 2004, S.O. 2004, c, 3, Sched A. (Online) Available:
  - http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm

- Canada. Parliament. House of Commons. Personal Information Protection and Electronic Documents Act, R.S.C. 2000, c-5. (Online) Available:
  - http://laws.justice.gc.ca/en/P-8.6/index.html

- Yamashita M, et al. Ontario Hospital Association (OHA). Ontario Hospital eHealth Council. Privacy and Security Working Group. Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals. July, 2003.

- COACH: Canada's Health Informatics Association. Security and Privacy Committee. Guidelines for the Protection of Health Information. May, 2001

- Ontario, Provincial Legislature, Mental Health Act, R.S.O. 1990

- Ontario, Provincial Legislature, Health Care Consent Act, R.S.O. 1996

- Accreditation Standard 12.2 The team meets applicable legislation for proteting the privacy and confidentiality of client information

8.0 Sponsor

Chief Privacy Officer

9.0 In Consultation with

Risk Management
Professional Advisory Committee
Medical Advisory Committee
Professional Advisory Committee
Executive Team
Hospital Legal Counsel

10.0 Posting Dates

Initial Posting Date:	04-04
Posting Date History:	02-07
	02-15

11.0 Attachments/Appendix

None