



Complete the following policy template. Do not delete unused sections of the template. Unused sections should remain blank.

Title: Privacy and confidentiality		<input checked="" type="checkbox"/> Policy <input type="checkbox"/> Policy & Procedure <input type="checkbox"/> Procedure Only <input type="checkbox"/> Protocol Only
Policy Type:		Category
Corporate		Privacy
Approval Authority: Choose an item.		
Date of Original Issue: July, 2021	Revised Date: May, 30, 2024	Next Review Date: May, 30, 2027
Distribution: <input checked="" type="checkbox"/> Hospital-Wide		
Related Policies: Complaints & Investigation Policy Release of Information and Correction Policy Breach Management Policy Consent Management Policy Logging and Auditing Policy Confidentiality Agreement Emailing Personal Health Information Policy		
Keywords: Privacy, Confidentiality, Personal Health Information, PHIPA, Privacy Breach		
NOTE: This is a CONTROLLED DOCUMENT. A printed copy of this document may not reflect the current version; always check against the electronic version prior to use.		

Purpose:

Sault Area Hospital (SAH) is committed to maintaining the privacy and confidentiality of personal health information, regardless of the medium; written, electronic or verbal. SAH respects the patient's right to privacy while assisting employees/health care providers to obtain personal health information in a respectful, caring manner in the completion of their job functions while acting within the required legislation. SAH will govern the collection, use, and disclosure of any personal health information as required by legislation, notably the *Personal Health Information Protection Act* (PHIPA) and the *Freedom of Information and Protection of Privacy Act* (FIPPA) or as outlined by this policy.

Scope:

This policy applies to all individuals handling personal information or personal health information on behalf of SAH, including but not limited to:

- Physicians
- Staff
- Volunteers
- Students

- Vendors

Definitions:

Collect: means to gather, acquire, receive or obtain Personal Information or Personal Health Information by any means from any source

Disclose: means to make Personal Information or Personal Health Information in the custody or under the control of a Health Information Custodian, available or to release it to another person

Hospital Staff: for the purposes of this Policy, includes any employee, member of the medical staff, board member, volunteer, student or person approved to provide services at/for the Sault Area Hospital,

Health Information Custodian: means a person or organization under PHIPA that is legally permitted to have custody or control of Personal Health Information as a result of performing their work. SAH is a Health Information Custodian.

Health Record

Any Record of Personal Health Information in any form. This includes electronic and physical files, email and other correspondence, audio, film, photographs, or other documentary material. Examples of a Health Record include:

- any report, document, information and other materials which pertains to the health status of an individual, whether produced by SAH or transferred from another institution to SAH
- diagnostic images and reports; or
- laboratory slides and reports.

Institution: means an organization under FIPPA that is legally permitted to have custody or control of Personal Information as a result of performing their work. SAH is an Institution.

Personal Health Information:

Any identifying information about an individual in oral or recorded form that:

- relates to the physical or mental health of an individual, including family health history,
- 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;
- is a plan of that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under the *Connecting Care Act, 2019*;
- relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual;
- 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;
- is the individual's health number;
- or identifies an individual's substitute decision-maker.

Personal Information

Any recorded information about an identifiable individual, including:

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

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;

Privacy Breach: An incident involving the unauthorized collection, use or disclosure of Personal Information or Personal Health Information

Record: A record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise noted

Use: means to view, handle or otherwise deal with Personal Information or Personal Health Information in the custody or under the control of a Health Information Custodian

ACCOUNTABILITY

The Chief Privacy Officer is accountable for overseeing the privacy and confidentiality of all personal health information at Sault Area Hospital. The Chief Privacy Officer or designated Privacy Officer will coordinate the investigation of all privacy breaches including any reporting to the Information and Privacy Commissioner of Ontario.

Department managers shall review any departmental specific information or procedures related to privacy and confidentiality with any Hospital Staff under their direct supervision.

It is a condition of employment and/or granting of hospital privileges that all Hospital Staff review the policies regarding access and confidentiality of patient information and sign the "Confidentiality Agreement" prior to receiving access to Personal Information and Personal Health Information, or performing duties as agreed within the Hospital.

A signed copy of the Confidentiality Agreement shall be maintained as follows:

- In the Human Resources Department for hospital employees, volunteers and students
- In the Medical Affairs Office for physicians and physician office employees
- In the Information Technology Department for employees of the Group Health Centre
- For external agencies other than the Group Health Centre, in the office of the appropriate Senior Manager for employees of other agencies carrying out duties at the Hospital
- In the Logistics Department for vendors

CONSEQUENCES FOR FAILURE TO COMPLY

Failure to abide by the provisions contained in this policy and/or under applicable legislation may result in disciplinary action up to and including termination of employment, and/or revoking hospital privileges or affiliation with the Hospital, as applicable. Failure to comply with privacy legislation can also expose individuals to personal liability and professional misconduct proceedings.

COLLECTION, USE AND DISCLOSURE

Patients will be informed of the SAH policies and procedures in the collection, use, access/disclosure of personal health information by making available a public statement and a patient information brochure. The Health Records Department is responsible for administering the public statement and patient information brochure.

Activities involving the collection, use and disclosure of personal health information may include the following:

- provide health care to the individual;
- assist the Hospital with obtaining payment for the treatment and care (from OHIP, WSIB, a private insurer or others) provided to the individual;
- plan, administer and manage the Hospital and its programs;
- conduct risk management activities;
- conduct quality improvement activities (such as sending an individual a patient satisfaction survey);
- provide education;
- conduct research that has been approved by the Research Ethics Board
- compile statistics;
- comply with legal and regulatory requirements

The patient's consent may be required for the collection, use, or disclosure of personal health information. Hospital Staff must ensure that they only collect, use and disclose personal health information as permitted or required by law.

Care providers must only collect the personal health information required to meet the purpose for which it is collected. Personal health information must be as accurate, complete, and up-to-date as possible. In the event that personal health information is to be used for a purpose not previously identified, unless law requires the new purpose, the consent of the individual is required before information can be used for that purpose.

CONSENT

Consent may be express or implied. Express consent is consent that has been clearly and explicitly provided. Implied consent is consent that a custodian concludes has been given based on the patient's conduct in the particular circumstances.

Where express consent is required, the Hospital requires that such express consent be documented in writing and be dated and signed by the individual providing consent.

An individual may withdraw consent, subject to legal restrictions.

Capacity to Consent

Patients are presumed to be capable of consenting to the collection, use or disclosure of personal information. A patient is capable of consenting to the collection, use or disclosure of personal health information if they are able: (i) to understand the information that is relevant to deciding whether to consent, and (ii) to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing consent.

There must be reasonable grounds to believe a patient is incapable of consent to the collection, use or disclosure of personal health information. A patient may be capable of consenting to the collection, use or disclosure of some parts of personal health information, but not others, or may be capable of consenting at one time, but incapable of consenting another time.

Requirements for Valid Consent

Where consent of a patient is required, consent must: (i) be consent of the individual (ii) be knowledgeable, meaning it is reasonable in the circumstances to believe that the patient knows the purpose of the collection, use or disclosure, as applicable, and that they may give or withhold consent, (iii) relate to the information, and (iv) not be obtained through deception or coercion.

Individuals Who May Consent

For patients capable of consenting, consent may be given by the patient or, if the patient is at least 16 years of age, any person whom the patient has authorized in writing to act on their behalf who is capable and at least 16 years of age.

For children who are less than 16 years of age, consent may be given by a parent of the child or a children's aid society or otherwise as permitted by law.

For patients incapable of consenting, the substitute decision-maker pursuant to applicable law.

For deceased patients, the estate trustee or the person reasonable for the administration of the estate.

When Consent is Required:

Express Consent is required when:

1. Personal health information is disclosed to:
 - Anyone other than the care providers currently involved in the care of the patient (circle of care).
 - Other third parties not directly involved in the care of the patient (e.g. includes lawyers, social agencies, insurance companies, adjusters on behalf of a patient claim or proceeding, police without a warrant, and Probation and Parole Services).
2. Personal health information is collected, used or disclosed for fundraising, marketing or market research, or for research purposes, unless otherwise permitted by law.

In such cases, the express consent of the patient/substitute decision-maker is required.

Consent can be implied when:

1. Personal health information is used or disclosed by Hospital Staff, including all employees, medical staff, students, allied health workers or other persons approved to provide service at/for Sault Area Hospital, who require the information in order to provide care to a patient or perform specific job functions (circle of care).
2. Personal health information is provided to another health information custodian for the purpose of providing or assisting in providing the patient with health care, for example:
 - Where employees of physicians' offices require the information to assist the physician in providing care for the patient, or the administrator/delegate of another health care facility or Nursing Home requires the information to provide ongoing diagnosis, treatment and care of a patient.

The circle of care does not include health care custodians who are *not* involved in the treatment of the patient, or any non-health care custodian (such as insurance companies).

Consent is not required where:

1. Disclosure is reasonably necessary for the provision of health care, and it is not reasonably possible to obtain a patient's consent in a timely manner, i.e. emergency situation.
2. Disclosure is required for the purpose of contacting a relative, friend or potential substitute decision-maker of a patient, if the patient is injured, incapacitated or ill and unable to give consent personally.

Disclosure is required to comply with legislation, court order or other legal proceedings such as:

- Chief Medical Officer of Health or Medical Officer of Health: Information to diagnose, investigate, prevent, treat or contain communicable diseases and SARS.
- Children's Aid Society: Information about a child in need of protection (e.g., abuse or neglect).
- College of a regulated health care professional where there are reasonable grounds to believe a health care professional has sexually abused a patient: Information and

- details regarding the allegation and the name of the health care professional. The name of the allegedly abused patient can only be provided with express consent.
 - College of Physicians and Surgeons of Ontario: Information about the care or treatment of a patient by the physician under investigation.
 - Coroner or designated Police Officer: Facts surrounding the death of an individual in prescribed circumstances (e.g., violence, negligence or malpractice), information about a patient who died while in the hospital after being transferred from a listed facility, institution or home and information requested for the purpose of an investigation.
 - Subpoena, order, warrant, writ, summons or other process issued by an Ontario court - Specific information outlined on the subpoena, warrant, summons, etc.
 - Workplace Safety and Insurance Board: Information the Board requires about a patient receiving benefits under the Workplace Safety and Insurance Act.
 - Cancer Care Ontario, Canadian Institute for Health Information, Institute for Clinical Evaluation Sciences or Pediatric Oncology Group of Ontario: To analyze or compile statistical information.
 - Individuals assessing patient capacity, not providing care to the patient to assess capacity under the Substitute Decisions Act, Health Care Consent Act, or PHIPA.
 - Public Guardian and Trustee, Children's Lawyer, Residential Placement Advisory Committee, Registrar of Adoption of Information, Children's Aid Societies to carry out their duties and, for the PGT, to investigate serious adverse harm resulting from alleged incapacity.
 - Public Guardian and Trustee (PGT) to investigate an allegation that a patient is unable to manage their property.
 - Police without a warrant where there are reasonable grounds to believe that disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm.
 - To assist police under the Missing Person Act in which the request must be directed to Health Records.
3. Personal health information is provided to a lawyer acting on behalf of SAH.
 4. Personal health information is provided to a researcher where the researcher provides a research plan that meets the requirements under PHIPA. In such cases the patient's name and any other means of identification of the patient must be removed.
 5. Collection, use or disclosure is authorized by the Information Privacy Commissioner of Ontario.
 6. There are reasonable and probable grounds to believe it is in the public interest to disclose the personal health information and the record reveals a grave environmental, health or safety hazard to the public. If practical, notice to the patient about the intention to release the record, a description of the contents of the record, and an invitation for the patient to provide representations on why the confirmation should not be disclosed will be provided.

ACCESS

Individual Access to Own Personal Information

1. A patient (or substitute decision-maker, as applicable) may access the patient's own personal health information. An individual is entitled to access except where granting such access could reasonably be expected to result in a risk of serious harm to the treatment or recovery of the individual or where access is prohibited by law.
2. All requests for access to personal health information shall be coordinated through the Health

Records Department.

- The request must be accompanied by an original copy of an authorization for release of information, signed by the patient/substitute decision maker and witnessed by another person.
 - The release shall include the name, address of the recipient of the information, the type of information requested, the date that the release is signed, as well as an expiry date. If no expiry date is provided, the authorization will remain valid for a period of 90 days from the date of signing.
 - All documents released from the health record are logged through Release of Information in the Meditech system.
 - The individual/agency to whom the information was released and the date released will be documented on the back of each health record.
 - A copy of the completed request and the signed consent will be placed in the health record or stored by Release of Information.
 - Access to the original health record by a patient/substitute decision maker shall be in the presence of a hospital designate to ensure that the integrity of the record is maintained.
3. The Medical Director of Mental Health will be consulted on all requests regarding release of Mental Health personal health information, and shall approve or deny access according to PHIPA and the Mental Health Act.
 4. If a patient feels the information in their personal health record is incorrect they shall be directed to the Manager of Health Records or Privacy Officer. The record must be corrected where the patient demonstrates that the record is incomplete or inaccurate for the purpose for which Sault Area Hospital used the record. Sault Area Hospital will not correct professional opinions made in good faith. In this case, the patient or substitute decision maker will be provided with the opportunity to write a letter detailing their issues with the health record. The letter will become part of the chart and with the patient and decision maker's consent will be copied to all who received a copy of the documentation.

Public and Media Inquiries

1. At the first reasonable opportunity following admission to the Hospital, patients will be provided with an Opt-Out Form to object to the disclosure of the fact that they are a patient at the Hospital, their general health status, and their location in the Hospital. If the patient does not specify any restrictions, consent is implied that they will allow SAH to confirm the patient's presence at SAH and disclose the patient's location should someone inquire at switchboard. Note that it is acceptable to disclose generic information as to the patient status (e.g. stable condition, critical condition) if the patient did not opt out for privacy purposes.
2. Further information will not be disclosed to the public or the media unless express patient consent is provided. All media inquiries will be addressed by the Communications/Public Affairs.
3. Personal health information is generally exempt from freedom of information requests under the *Freedom of Information Act*. Freedom of information requests will be addressed by the Privacy Officer in accordance with applicable legislation.

Voice Messaging

Reminder calls to patients for upcoming appointments may be necessary. When leaving a voice message on an answering machine, or with a third party, staff shall exercise caution regarding the content of any messages left for patients. While it is acceptable for messages to contain the name and contact information of a department, messages should not contain any personal health information of the patient, regarding the nature of the appointment. It is always best practice to obtain consent from the patient prior to leaving any future voicemails.

Retention of Personal Information

Personal health information will be retained only as long as necessary for the fulfillment of health care services or as otherwise required under applicable legislation including the *Public Hospitals Act*. Personal health information will be stored, retained and destroyed as per the Record Retention, Storage and Destruction Policy.

SAFEGUARDS FOR PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

1. Security rights to electronic records shall be restricted based on the role of the health provider. If an exception is required, the Information Systems Request Form must be completed by the authorizing individual and forwarded to I.T.

Requesting access/disclosure for	Approval authority
Staff, Volunteers, Clinical Students	Manager
Nursing Students	Chief Nursing Executive
Manager, Director, Senior Manager	Supervisor
Employees of Other Agencies	Senior Manager Responsible
Medical Staff/Students and Physician Office Employees	Chief of Staff/Delegate

2. Where personal information and personal health information has been collected, users shall respect the integrity of the data on the hospital's information system by:
 - Protecting the secrecy and integrity of the password or access code.
 - Encrypting patient information that is stored on portable devices.
 - Not using another user name and password to gain access to an application or data.
 - Not copying or modifying files belonging to other users.
 - Not copying hospital software or data entrusted to them.
 - Not attempting to install any software without involvement/permission of the Information Technology Department.
 - Not copying and pasting personal health information from any system to e-mail and/or print to others.
3. Affiliation agreements will include provisions for maintaining confidentiality and protection of privacy.
4. All new projects are required to determine the need for a Privacy Impact Assessment during the planning phase of the project.
5. Only information that is immediately necessary for the continuity of patient care shall be transmitted by fax. Refer to the Privacy Procedure for Transmission of Health Information by Fax for specific requirements. Information can also be shared through electronic means, such as a secure file transfer, as long as has been approved by IT.
6. *External e-mail must only be used to transmit personal health information outside of the organization as per the guidelines set in SAH's Emailing Personal Health Information policy.*
7. Web based file storage or cloud services not managed by SAH (e.g. Apple's iCloud, Google's Cloud) must never be used to store sensitive information, including but not limited to personal health information and personal information.

Printing or Removing Personal Information or Personal Health Information from SAH

Printing or removing personal information or personal health information from SAH premises is prohibited unless

the following conditions are met:

- It is mandatory for urgent patient care and/or;
- It has been approved by the department manager or SAH's Privacy Office.
- By email, the department manager will inform the Privacy Office that approval has been granted. The email must contain details about the request and the necessity of the approval.

Printing or removing personal information or personal health information from SAH premises increases the probability of a privacy breach. In addition to the safeguards found in this policy, further physical safeguards listed below must be utilized:

- It is not an original document;
- Secure transportation by means of enclosed briefcase or that of similar security;
- Direct transportation to a secured environment (example: home office) and not left unattended during transportation;
- Maintained in a locked filing cabinet inaccessible to others;
- Returned immediately after use to SAH to be securely shredded.

TRACKING AND MONITORING

Compliance with SAH Privacy Policies and Procedures

Audits to determine whether there has been a violation of access will be coordinated by the Privacy Officer. Audits may be requested by anyone who believes that patient health information has been inappropriately accessed. Staff members requesting an audit must submit the request for audit to their manager. Patients or substitute decision-makers requesting audits should be referred to the Privacy Officer.

Privacy Breach

Breaches of privacy are contrary to the Sault Area Hospital iCare values. An electronic occurrence report must be completed for each confirmed privacy breach.

Please refer to Privacy Procedure – Complaints and Investigation 1-140. All potential and actual privacy breaches must be forwarded to the Privacy Officer for investigation. These include but are not limited to the following:

1. Accessing patient or health information when it is not required to provide care to a patient or in the performance of duties.

Examples of access considered to be a breach of confidentiality include:

- Accessing the health record of oneself other than through the Health Records Department
- Accessing the health record of a staff member, family member, friend, or anyone for whom you do not have a requirement to view information based on providing care or performing duties
- Accessing any patient information (address, date of birth, next of kin, etc.) for staff members, family member, friend, or anyone for whom you do not have a requirement to view information based on providing care or performing duties
- Sharing of patient information via social networking (i.e. Facebook, Hotmail, Twitter, MSN)

2. Discussing patient information that has come to your attention by virtue of being involved in the care of a patient or being an employee, medical staff, or other person affiliated with the hospital, with:

- Another person who is not involved in the care of the patient or does not require the information to perform job functions, or
 - Within range of other people who should not have access to the information.
3. Removal, copying or transmittal of patient information, other than through those procedures outlined in the Privacy Procedure "Transmission of Health Information by Facsimile" and for reasons other than communication with persons involved in the care of the patient or requiring information in the performance of duties.
 4. Leaving patient information in unattended or unsecure locations where it may be accessed by unauthorized person.

Supportive Data / Definitions:

Terminology: Definition	
Terminology: Definition	Terminology: Definition
Terminology: Definition	Terminology: Definition

References:

Revision History:

Date:	Signing Authority: Name / Title
May 30, 2024	Lucas Febbraro, Privacy Officer
July 25, 2024	Wishart Law Firm and Lucas Febbraro, Privacy Officer

