SUBJECT:	**PRIVACY AND CONFIDENTIALITY**
APPLIES TO:	All Staff, Physicians, Volunteers, and Students, Visitors, Vendors, Consultants
AUTHORIZED BY:	VP Innovation, Quality & Medicine
CATEGORY:	Privacy and Information Technology
REPLACES:	Confidentiality 7.10 (September 2016)

POLICY

Sault Area Hospital is committed to maintaining the confidentiality of personal health information, regardless of the medium; written, electronic or verbal. The Hospital respects the patient's right to privacy while assisting employees/health care providers to obtain patient and health information in a respectful, caring manner in the completion of their job functions. It is therefore the policy of SAH that no one shall collect, use or provide access to any personal health information, or to improve the quality of care, except as needed for the health care of an individual, as required by legislation, or as outlined by this policy.

DEFINITIONS

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, is a plan of service within the meaning of the *Long-Term Care Act, 1994*, relates to payments or eligibility for health care, 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 Health Information Protection Act (2004).*

Personal Information

Any recorded information about an identifiable individual as per the *Freedom of Information Protection of Privacy Act*, 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; ("renseignements personnels").

Health Record
The health record is comprised of any report, document, information and other materials produced by hospital staff which pertains to the health status of an individual, as well as diagnostic images and reports and laboratory slides and reports. It also includes any reports or consultations performed at another institution while the individual was a patient at the Sault Area Hospital, or sent from another institution with a patient who is to be admitted to or treated at the Sault Area Hospital. The health record is maintained for the purpose of documenting the details of an individual's health care and to provide a medium of communication among health care providers. The health record is the property of Sault Area Hospital.

Consent
Consent must be consent of the individual, must be knowledgeable, must relate to the information, and must not be obtained through deception or coercion. *Personal Health Information Protection Act, 2004*

Privacy Breach
An incident involving the unauthorized collection, use or disclosure of personal health information. An electronic occurrence report must be completed for each confirmed privacy breach.

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 confidentiality with a new employee.

It is a condition of employment/granting of hospital privileges that all staff, including employees, members of the medical staff, board members, volunteers, students or persons approved to provide services at/for the Sault Area Hospital, review the policies regarding access and confidentiality of patient information and sign the "Confidentiality Agreement" prior to receiving access to information or records, 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 office of the appropriate Senior Manager for employees of other agencies
- In the Information Technology Department for employees of the Group Health Centre
- In the Logistics Department for vendors

Failure to abide by the provisions contained herein will result in disciplinary action up to and including suspension, termination of employment, hospital privileges or affiliation with the Hospital, as applicable.

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 patient's consent is required for the collection, use, or disclosure of personal health information. An individual may withdraw consent, subject to legal restrictions. Consent is not required if there is no time to obtain consent, i.e. emergency situation.

Caregivers 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.

As your hospital duties require, you are specifically authorized to collect and use personal health information from an individual to whom the information pertains as required in order to:

- 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);
- teach;
- conduct research that has been approved by the Research Ethics Board
- compile statistics;
- comply with legal and regulatory requirements;

Consent

Consent is required when:

1. Personal health information is disclosed to:
    - Physicians other than the attending or those 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).

In such cases, the express consent of the patient/substitute decision-maker is required. Consent for disclosure must be:

- In writing
- Dated no more than 3 months prior
- Signed

2. Personal health information is disclosed to:
    - Any other person with the consent of the patient, if the patient is considered to be competent for this purpose and has signed a consent form.
    - To any other person with the consent of the appropriate substitute decision-maker, where the patient is not mentally competent and the substitute decision-maker has signed a consent form.

Consent is not required 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. Employees of physicians' offices require the information to assist the physician in providing care for the patient.

3. Administrator/delegate of another health care facility or Nursing Home requires the information to provide ongoing diagnosis, treatment and care of a patient.

4. Personal health information is required to comply with legislation, is requested by court order or subpoenaed for 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, name of the health care professional and name of the allegedly abused patient. The patient's name can only be provided with 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.

5. Personal health information is provided to the personal representative of a patient who has died.

6. Personal health information is provided to a lawyer acting for the health care facility.

7. Personal health information is provided to a person determining capacity for treatment, admission to a care facility or personal assistance services.

8. Personal health information is provided to any person, for research, process improvement, academic pursuits or the compilation of statistical data. In such cases the patient's name and any other means of identification of the patient must be removed.

9. The Information Privacy Commissioner of Ontario authorizes the collection of personal health information.

Access

Individual Access to Own Personal Information

1. Personal health information may be accessed by a patient/substitute decision-maker. 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 the 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. 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. Alerts will be recorded in the Admissions System for patients who do not wish to have visitors or phone calls. If the patient does not specify any restrictions, consent is implied that he/she will allow SAH to disclose the patient's room number. 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 media unless patient consent is provided. In such situations, media inquiries will be addressed by the Communications/Public Affairs.

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.

Retention of Personal Information

Personal health information will be retained only as long as necessary for the fulfillment of those purposes. 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 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.

6. *External e-mail must not be used to transmit personal health information. The only time personal* health information (PHI) can be sent is from a Sault Area Hospital account via ONE Mail which both parties must be subscribers. This includes mobile computing devices.

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 shred.

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.

Unauthorized Disclosure/Breach of Confidentiality
Breach of confidentiality is contrary to the Sault Area Hospital iCcare values. 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 persons.

RELATED RESOURCES

1. Privacy Procedure – Complaints & Investigation
2. Privacy Procedure – Transmission of Personal Health Information by Fax (Administrative Procedure)
3. Remote Access to Patient Information
4. Internet Access
5. Record Retention, Storage and Destruction
6. Guidelines for Access to Hospital Information Systems
7. Request for Audit Form
8. Authorization for Release of Health Records
9. Privacy Breach Checklist and Review
10. Confidentiality Agreement