		POLICY No:	I-i-80-95
TITLE:	Privacy Policy	**ORIGINAL ISSUE DATE:**	August 17, 2016
		EFFECTIVE DATE:	August 17, 2016
ISSUED BY:	Privacy Office	**REVISION DATE:**	
APPROVED BY:	Executive Council	**NEXT REVIEW DATE:**	August 17, 2019

TABLE OF CONTENTS

TITLE	**PAGE**
Purpose and Scope	**1**
Definitions	**2**
A. Capacity to Consent to the Collection, Use and Disclosure of PHI	**3**
B. Consent to Collect, Use or Disclose PHI	**4**
C. Authority to Collect PHI Without Consent	**6**
D. Authority to Use PHI Without Consent	**6**
E. Authority to Disclose PHI Without Consent	**8**
F. Fundraising	**11**
G. Media	**11**
H. Telephone Inquiries	**11**
I. Patients Requesting Restricted Access to their PHI ("Consent Directive" or "Lockbox")	**13**
J. Secure Disposal of PHI	**14**

PURPOSE AND SCOPE

The purpose of this policy is to assert Sinai Health System's ("Hospital") commitment to the protection of personal health information ("PHI") from unauthorized collection, access, use, or disclosure, and protection of PHI from theft or loss. This policy addresses the appropriate collection, use and disclosure of PHI, the patient's right to limit access to his/her medical record, and the secure disposal of PHI when it is no longer required.

1) The Hospital recognizes its obligation to respect privacy and is committed to maintaining the confidentiality of PHI, whether written, verbal, electronic, photographic or stored on any other medium.

2) The Hospital recognizes its obligation to ensure and facilitate timely access to information as required by authorized individuals for direct patient care, administrative use, or where required to do so by law.

3) To assist with meeting our privacy obligations, the Hospital has designated a contact person, the Corporate Privacy Officer, who is accountable for the Hospital's compliance with its own policies and applicable privacy legislation.

4) It is the legal, professional and ethical duty of all persons affiliated with Sinai Health System to keep private the information they receive from and about patients. This duty arises from the recognition that capable patients have the right to control the collection, use and disclosure of their PHI, including the right to determine the time and manner in which the disclosure of such information may occur to third parties, including care providers, family members, friends and others.

5) Accordingly, it is the obligation of all of those who collect, receive and share confidential information concerning patients at Sinai Health System to exercise the utmost vigilance in the protection of patient privacy.

DEFINITIONS

"**Patient health information**" or "**personal health information**" ("**PHI**") is identifying information about an individual in oral or recorded form, if the information:

- relates to the physical or mental health of the individual, including the individual's medical history and the individual's family 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;
- relates to payment or eligibility for health care;
- is the individual's health number;
- identifies an individual's substitute decision-maker; or
- Donations of body parts and substances, including information derived from testing or examination of such parts or substances.

  Any other information about an individual that is included in a record containing PHI is also part of this definition. It is not necessary for the individual to be actually named for the information to be considered PHI.

"**Collect**" means to gather, acquire, receive or obtain the information by any means from any source.

"**Use**" means to handle or deal with the information, and includes accessing PHI for viewing purposes only.

"**Disclose**" means to make the information available or to release it to another person or organization.

A. Capacity to Consent to the Collection, Use and Disclosure of PHI

1) An individual is incapable of consenting when the individual is not able to do either of the following:

   a) Understand the information needed to make a decision on whether or not he/she should consent to the collection, use or disclosure of PHI; and
   b) Appreciate the consequences of giving, withholding or withdrawing consent.

2) There is no age of capacity to consent. The test for capacity to consent is the same regardless of a patient's age, although age may impact upon a patient's ability to understand or appreciate.

3) Capacity may vary with time. For example, a patient may be incapable of deciding how his/her PHI should be used at the time of admission, but regain capacity with treatment.

4) Capacity may vary depending on the PHI decision at issue. For example, a patient may be capable of deciding to disclose certain aspects of his/her PHI to certain persons, but lack the ability to appreciate the consequences of withholding consent to disclose his/her PHI to other persons.

5) It is the responsibility of the individual proposing to collect, use or disclose PHI to review a patient's capacity, and obtain consent as required.

6) You may presume an individual is capable of consenting unless you have reason to believe otherwise.

7) If you determine that a patient lacks the capacity to consent, you must:

   a) notify the patient of your finding;
   b) advise the patient that they have a right to challenge your finding by requesting a Consent and Capacity Board hearing; and
   c) document your capacity assessment and the notice provided to the patient in the patient's health record.

   If the patient is a psychiatric patient under the *Mental Health Act*, additional requirements apply in respect of notice and rights advice.

8) Where a patient is incapable of making a decision about the collection, use or disclosure of his/her PHI, you must obtain the consent of the patient's substitute decision-maker's ("SDM"). The SDM must be at least 16 years old, capable, willing, available, and not prevented by court order from accessing the patient. Ranking of SDMs is determined in accordance with the "Consent to Treatment Policy" Policy #: III-H-5-20, in the General Manual.

9) Where a patient is incapable with respect to a treatment, the patient's SDM for treatment purposes is deemed to be the SDM in respect of PHI to the extent that it is necessary or ancillary to the treatment decision(s) for which the patient is incapable.

B. Consent to Collect, Use or Disclose PHI

1) The knowledgeable consent of the patient is required for the collection, use or disclosure of their PHI. An individual's consent is knowledgeable if he/she:
   a) understands the purpose of the requested collection, use or disclosure, and
   b) understands that he/she may give or withhold consent.

2) Consent may be withdrawn at any time, but the withdrawal does not have a retroactive effect.

3) The patient may attach conditions to their consent to collect, use or disclose his/her PHI, but not to the extent that it interferes with a health care provider's legal and professional documentation requirements.

4) Consent does not always need to be in written form; it can be obtained verbally and that fact recorded in the individual's health record by noting the date and time; to what the consent relates (eg. collecting, using or disclosing what specific PHI); the purpose of the collection, use or disclosure; and any other relevant details.

5) When you elect to obtain a signed consent, have the patient complete and sign the "Consent for Disclosure of Personal Health Information".

6) Consent can sometimes be implicit rather than explicit. If you receive PHI for the purpose of providing or assisting in the provision of care, you are entitled to assume you have the patient's consent to collect, use or disclose the PHI for the purpose of providing care, unless you are aware that the consent to do so has been withdrawn or withheld by the patient.

7) If a patient instructs you not to disclose all relevant PHI to another healthcare provider that you would have considered necessary to disclose in the circumstances, then you must notify the recipient of the fact that you do not have the patient's consent to disclose all relevant PHI.

8) Consent must be explicit (i.e. verbal and documented in health record by staff, or consent form signed by the patient) where a disclosure is being made to someone who is not a health care provider (e.g. to a patient's family member).

9) There are some exceptions to the general rule that a patient's consent must be obtained prior to collecting, using or disclosing PHI. These exceptions are reviewed below in sections (C), (D) and (E). Except where the use, collection or disclosure of PHI without consent is permitted, consent should be sought and documented prior to the collection, use or disclosure of PHI.

10) In deciding whether to obtain an individual's explicit or implicit, written or verbal consent, you should exercise professional judgment, discuss the decision with your peers and supervisor, and/or consult with the Privacy Office at ext. 2101.

C. Authority to Collect PHI Without Consent

1) PHI should always be collected directly from the patient whenever possible, with their consent. It is permissible to obtain PHI directly from a patient without their consent if the information is required to provide care and time is of the essence.

2) If you have a concern about the accuracy, completeness or timeliness of the PHI provided directly from the patient to whom the PHI pertains, you may obtain the information from another source, such as a knowledgeable person, health care practitioner or institution, without the patient's consent.

3) You should only collect as much PHI as is necessary to accomplish the purpose for which you are collecting it. Do not collect more PHI than you need.

4) If you wish to use photography or audio/visual recording in the course of providing patient care, consult the Hospital policy on Photography and Audio-Visual recording.

D. Authority to Use PHI Without Consent

1) As part of your association with the Hospital, you have the authority to access and use certain PHI. This access must be limited, and strictly confined, to information required to assist in providing patient care.

2) In so far as your Hospital duties require, you are specifically authorized to use a patient's PHI as required in order to:

a) provide health care to the individual, except to the extent that the individual has restricted access to their PHI (see section (H) below);
b) assist the Hospital with obtaining payment for the treatment and care (e.g. from OHIP, WSIB, or a private insurer) provided to the individual;
c) plan, administer and manage the Hospital and its programs;
d) conduct risk management activities;
e) conduct quality improvement activities;
f) educate medical trainees to provide care;
g) conduct research that has been approved by the Research Ethics Board, but only in accordance with the research plan approved by the Sinai Health System Research Ethics Board; and
h) comply with legal and regulatory requirements.

In order to access or use PHI to for risk management, quality improvement or education functions, the use must fall within your official duties, be described in a contract with the Hospital or be specifically authorized by your supervisor. If you have any questions about your authority to use a patient's PHI without consent, consult your supervisor or the Privacy Office at ext. 2101.

3) Hospital staff are not permitted to use PHI for fundraising purposes.

4) Shared systems that store PHI, such as ConnectingGTA or Patient Results Online (PRO), may only be used for direct patient care purposes. Shared systems may not be accessed for quality improvement, education or research purposes.

5) In the clinical context, it is recognized that it will often be necessary to share PHI with other members of the health care team, that is, those individuals within the patient's "circle of care." This should only occur when sharing PHI is necessary to advance the therapeutic interests of the patient. Judgments about sharing PHI within the circle of care must be made by members of the health care team, guided by a good faith belief as to what is in the best therapeutic interests of the patient. Information should not be shared unless there is a legitimate need to know. Care should be taken to ensure that PHI is not used or accessed by non-treating personnel or others without a legitimate need to know.

6) Authorization may be given to external agents and partners to use PHI in order to assist the Hospital with fulfilling its mission. For example, PHI is sometimes shared with outside companies, like the companies that provide the Hospital with our electronic health record, transcription services and equipment maintenance services, or representatives of certain companies may be exposed to PHI by virtue of their presence at the Hospital, like the security guards who patrol the Hospital premises. It is the responsibility of the Manager of the department and the responsible Vice-President who oversees the negotiation of the Hospital's agreement with the external agent, in consultation with the Privacy Office, to ensure that the external agent and its representatives are contractually bound to adhere to our privacy requirements, have signed a confidentiality agreement, and/or have undergone privacy training, as the circumstances may require. Extra care should be taken when working with foreign partner companies to ensure that they appreciate their privacy obligations under the laws of Ontario. Conformity to the laws of other jurisdictions does not necessarily result in compliance with applicable Ontario privacy legislation.

7) When information is routinely shared with other health care organizations, like another hospital, the Ministry of Health and Long-Term Care, or Cancer Care Ontario, a written Data Sharing

Agreement ("DSA") should be entered into between all parties to confirm when, how and for what purpose information is being shared. Contact the Privacy Office for further guidance.

8) You are encouraged to use the services of Shared Health Supply Services (SHSS) to assist with your contract negotiations as they are knowledgeable about, among other things, the Hospital's privacy obligations in respect of vendors or, alternatively, contact the Privacy Office or Legal Counsel for assistance with preparing an agreement when SHSS is not involved in the process.

9) Access to your own health record while in the Hospital or after discharge must be done in accordance with the "Confidentiality and Release of Information," Policy #:VII-S, in the Health Records Services Manual (http://info/ReleaseOfInformation/MSH_Policy.htm). You are not permitted to use your access to the Hospital's PHI systems to access your own health record.

E. Authority to Disclose PHI Without Consent

1) Disclosure of PHI is prohibited without the patient's consent, except in the circumstances listed below. Note that these exceptions permit, but do not require, PHI to be disclosed without consent. Professional judgment, consultation with your supervisor and/or the Privacy Office should guide the use of discretion in disclosing PHI without patient consent.

   a) Unless the patient has expressly instructed otherwise, PHI may be disclosed to a health care provider or facility where the provider and recipient of the PHI currently provide, or assist in the provision of health care, or have done so in the past. The purpose of disclosure must be to maintain or improve the quality of care provided to the patient or similar patients.

   b) To locate a friend, relative or potential SDM if the patient is incapacitated and unable to give consent.

   c) To determine, assess or confirm capacity to consent.

   d) To the Public Guardian and Trustee, Office of the Children's Lawyer, Children's Aid Society or a Residential Placement Advisory Committee under the *Child and Family Services Act*.

e) If a patient is being lawfully detained (e.g. pursuant to a Form 3 or 4 under the *Mental Health Act*), to assist in making arrangements for the provision of health care, or assist in making a decision concerning the placement or appropriate disposition of a patient detained under the *Mental Health Act, Child and Family Services Act* or Part 20.1 (Mental Disorders) of the *Criminal Co*de.

f) To determine eligibility for goods, services or benefits funded by the federal, provincial or municipal government, or the LHIN.

g) As required by statute. For example, to the Children's Aid Society as required by the *Child and Family Services Act*, to the police as required by the *Mandatory Gunshot Reporting Act*, or to Public Health as required by the *Health Protection and Promotion Act*.

h) If the disclosure is to another non-treating health care provider, it is reasonably necessary to disclose the PHI in order to provide health care to the individual, and it is not possible to obtain the individual's consent in a timely manner, unless the patient specifically instructed not to make the disclosure.

i) When disclosing PHI will eliminate or reduce a significant risk of serious bodily harm to a patient or third party. The first concern of the health care professional must be the safety of the patient or third party. Even when the health care professional is confronted with the necessity to disclose, confidentiality should be preserved to the maximum possible extent.

j) Pursuant to a court order, summons, subpoena or warrant. In all instances, upon receipt of such a document, you should consult with the Office of the General Counsel to ensure that the document legally authorizes the disclosure.

k) To inform next of kin about a patient's death.

l) To a person carrying out an investigation that is authorized by statute or warrant, such as the police. In communicating with police, note the following:

   i. Always document the Officer's name, division number, badge number, and telephone number. The nature/reason for the request must also be documented (i.e. motor vehicle accident).

ii. Staff should ask the officer to complete a Police/Authority Request for Information Form and provide the form to their manager for follow up.

iii. If the communication is by telephone, confirm the person on the other line is a police officer by asking for a telephone number and calling them back.

iv. Always consult your manager, Risk Management or the Privacy Office before any materials are accepted or any information is provided to a police officer;

v. In order for personal health information to be released, the Police Office must present one of the following documents: a valid court order, a search warrant, a subpoena, a coroner's write or an original written authorization of the patient allowing the release of the information requested. In all instances, upon receipt of such a document, you should consult with the Office of the General Counsel or Risk Management to ensure that the document legally authorizes the disclosure.

vi. **In situations where there is a risk of serious bodily harm** to a person or group of persons, provide the information that is necessary (and no more) to alleviate the risk of harm that and fulfill the purpose of the request.

vii. When asked if a John Doe is present at the Hospital, it is acceptable to reply with "yes" or "no".

2) All inquiries for PHI which are not dealt with in this section should be referred to the Privacy Office and/or the Office of Risk Management.

3) Every effort should be made to ensure that PHI is not inadvertently disclosed to persons not otherwise entitled to receive such information.

4) Subject to the reasonable limits, PHI should never be discussed in any area where others not entitled to receive that information are present, such as in elevators, washrooms, lounges, the cafeteria, at home or in public places outside the Hospital.

5) Because the Hospital is a teaching institution, opportunities may arise where the safeguarding of PHI will require extra vigilance. In the presentation of grand rounds, lectures or seminars, the identity of patients should not be revealed on or determinable from slides or radiological images. Except with prior written patient consent, under no circumstances should sufficient information be revealed to enable the identification of the patient.

6) In the presentation of case studies at external events such as conferences, extra vigilance should be taken to ensure that the identity of patients is not revealed or determinable from presentation materials. All presentation material must be reviewed prior to any presentation to ensure the absence of PHI or identifying personal information. Contact the Privacy Office for assistance as appropriate.

7) PHI should not be left in written form or displayed on computer terminals in locations where it may be seen by unauthorized persons (e.g., while transporting patients and their records through the Hospital, documents on a photocopier or fax machine, or at an unattended computer terminal).

8) Whiteboards should be placed in areas where patient and public access is restricted, balancing clinical and privacy objectives. Discretion should be used in determining what information is placed on whiteboards, balancing clinical and privacy objectives.

F. Fundraising

1) The Hospital releases patient names and mailing addresses to the Sinai Health System Foundation ("the Foundation"), with the implied consent of patients, unless a patient instructs otherwise.

2) This information shall be handled in accordance with the Information Sharing Agreement between the Hospital and the Foundation, and appropriate Foundation policies and codes of ethics (see Foundation policies on Patient Solicitation, Patient Mail, Patient Telemarketing, and Grateful Patient Program Procedures).

3) Patient information other than name and mailing address may not be released to the Foundation without the patient's prior written consent.

4) Hospital staff are <u>not</u> permitted to use PHI for fundraising purposes.

G. Media

1) All inquiries from the media, regardless of their nature, should be immediately referred to Communications. After business hours, a representative from this department may be reached through Locating.

2) Any release of information to the media must be done in accordance with the Hospital Media Policy in the General Manual and must not include any PHI without the patient's prior written consent.

H. Telephone Inquiries

1) It is the patient's right to keep his/her name out of the Hospital's Patient Directory.

2) When a patient requests that his/her name be removed from the Directory, this instruction must be noted by the Admitting Clerk and indicated in Flex Inquiry and PowerChart under the Patient Demographics tab, Privacy Alert. If a patient makes a request to not have their presence in the Hospital disclosed to callers, the Admitting department should be contacted to ensure the patient's preference is appropriately followed.

3) All staff must respect the patient's wishes in this regard by not confirming the patient's presence in the Hospital, without the patient's express consent.

4) For all other patients, you may confirm the patient's presence in the Hospital to those who telephone inquiring about the patient, and in addition to the patient's location in the Hospital, you may disclose his/her general health status in accordance with the following terms and definitions:

Good Vital signs are stable and within normal limits. Patient is conscious and comfortable and his/her prognosis is good or excellent

Fair Vital signs give no cause for concern. Patient is conscious, the prognosis is favorable, but he/she may be uncomfortable or have minor complications.

Serious Acutely ill with questionable prognosis. Vital signs may be unstable or not within normal limits. There is a chance for improved prognosis.

Critical Questionable prognosis. Vital signs may be unstable or not within normal limits. There are major complications and death may be imminent.

Patient consent (written or verbal) is required to disclose any additional information, including to family members.

5) Patients should be encouraged to appoint a family representative to whom more detailed information may be disclosed. The name of the family representative must be noted in the patient's health record and shared with all of the members of the health care team. Other family members telephoning or asking for more information in person should be directed to the family representative.

I. Patients Requesting Restricted Access to their PHI ("Consent Directive" or "Lockbox")

1) Patients have the right to limit or restrict how their PHI may be used or disclosed for healthcare purposes. In some cases, a patient may not want part of his/her PHI to be used by Hospital staff or disclosed to non-Hospital clinicians, such as a primary care provider or another Hospital.

2) Patients making a request to restrict access to their PHI should be counseled about the clinical risks (if any) associated with their particular request. Clinicians should document this discussion in the patient's health record, including the clinical risks associated with the request that were discussed with the patient. In addition, the patient should be provided with the Hospital's brochure, "Privacy: How to Limit the Use and Sharing of Your Personal Health Information" and instructed to contact the Privacy Office with respect to their request.

3) When the patient's request is accepted, with respect to the paper health record, there will be a form at the front of the paper record describing the patient's instruction as to what information you may not use or disclose. The 'locked' information will be kept in a sealed envelope in the paper record or, depending on the size of the request, the entire record may be 'locked' from use. With respect to the electronic record, a 'flag' will inform you that there is a 'lock' on information stored electronically.

4) In limited circumstances, the Hospital may deny a patient's request, such as where it conflicts with the law.

5) Even when a patient's request to "lock" information has been implemented, it may be over-ridden or temporarily ignored in the following circumstances:

a) With the patient's express, documented consent;
b) To comply with legal obligations such as reporting to a Children's Aid Society, reporting that a person is being treated for a gunshot wound, or to report certain diseases to Public Health;
c) For permitted uses such as risk management, healthcare planning or quality improvement purposes; or
d) To eliminate or reduce a significant risk of serious bodily harm to the patient or to others, like for the purposes of a Code Yellow or in response to a clinical emergency.

Anyone who accesses "locked" information must document their reason for doing so on the Lock Box Viewing Log, and the patient will be notified of the override by the Privacy Office.

6) In cases where a 'lock' exists, the health care team may not be able to consult certain information or encounters in the patient's record while providing care. Also, a complete record may not be released to another healthcare organization without express, documented consent.

J. Secure Disposal of PHI

1) All electronic and digital records containing PHI must be physically destroyed or magnetically erased. For example, CDs, videotapes, microfilm, and diskettes must be broken. Encrypting or overwriting the information is insufficient because it is possible that the information may be recovered at some time in the future, even if the keys have been destroyed in the case of encrypted information.

2) For the safe destruction of PHI stored digitally or electronically on a medium that cannot be destroyed, utilities must be used that are capable of removing all data from the medium rendering its reconstruction impossible. Questions and requests for assistance in this regard should be directed to Information Technology.

3) PHI must never be stored on a personal computer or mobile device, even temporarily, because even when the information appears to be deleted, utility programs can be used to reconstruct the deleted information. If you have mistakenly stored PHI on a personal computer, contact Information Technology to make arrangements for the cleaning of the hard drive.

4) All documents containing PHI must be discarded into the designated Shred-it containers. PHI cannot be discarded with regular garbage or in a recycling bin.

RELATED POLICIES

Acceptable Use of Information and Information Technology

Video and Photographic Images Policy

Privacy Incident Protocol

Confidentiality and Release of Information

REB Operating Procedures

For the Privacy of Employee information, see Confidentiality of Employee Information Policy