



TITLE: Privacy Policy: Protecting Personal Health Information at the Niagara Health System	POLICY
---	---------------

DOCUMENT NUMBER: 332-005-017	FILE NAME:
SECTION: Information Management SUBSECTION: Privacy, Data Protection & Security-PHI	EFFECTIVE DATE: 15/12/04 (DD/MM/YY)
APPROVED BY: Chief Privacy Officer/Lead, E-Health VP Clinical Services	REVISION DATE: 24/03/09 (DD/MM/YY)
	PAGE 1 OF 6

1.0 Purpose

At the Niagara Health System (NHS) privacy is governed by the (Ontario) Personal Health Information Protection Act, a law that establishes rules concerning the collection, use and disclosure of personal health information. As a health information custodian (HIC), the NHS and its agents (including staff, physicians, students and volunteers) are responsible for ensuring that the personal health information (PHI) of our patients is treated with respect and sensitivity.

2.0 Scope

This policy applies to all personnel at all NHS hospital sites.

3.0 Definitions

NHS – Niagara Health System, all hospital sites.

Agent – in relation to a health information custodian, means a person hat, 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. (PHIPA 2004, Definitions 2).

- Examples of agents of the NHS include, but area not limited to: employees, volunteers, students, physicians, residents, fellows, consultants, researchers, vendors.

HIC - Health Information Custodian – Listed persons or organizations under the Personal Health Information Protection Act such as hospitals, who have custody or control of personal health information as a result of the work they do. As a public hospital, the NHS is considered to be a Health Information Custodian (Personal Health Information Protection Act, 2004, s 3).

PHI – Personal Health Information – Information about an individual whether living or deceased, and whether in oral or recorded form, if the information

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family,
- 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 service within the meaning of the Long-Term Care Act, 1994 for the individual,
- 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. 2004, c.3, Sched. A, s.4(1); 2007,c.10, Sched.H, s.2.

Identifying Information:

means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual. 2004, c.3, Sched. A, s. 4 (2).

- **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.

3.0 Policy

The NHS is responsible for personal health information under its control in compliance with the (Ontario) Personal Health Information Protection Act (PHIPA), 2004.

- Accountability for NHS compliance with the policy rests with the President and Chief Executive Officer, although other individuals within the NHS are responsible for the day-to-day collection and processing of personal health information. In addition, other individuals within NHS are delegated to act on behalf of the Chief Executive Officer, such as the designated privacy contact person, the Chief Privacy Officer.
- NHS is responsible for personal health information in its possession or custody, including information that has been transferred to an agent of the NHS. NHS will use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
- NHS has implemented policies and practices to give effect to this policy, including:
 - a. Procedures to protect personal health information.
 - b. Signing of Confidentiality Statement (form 900063) by all agents of the NHS prior to commencement of employment or affiliation with the NHS
 - c. Procedures to receive and respond to complaints and inquiries about the NHS information practices.
 - d. Training staff and communicating to staff and other agents on information about PHIPA and NHS policies and practices.
 - e. Responding to requests for access to, or corrections of, personal health information in the custody of the NHS.
- In compliance with the Personal Health Information Protection Act, NHS will inform patients of the loss, theft or inappropriate access or disclosure of their PHI as soon as reasonably possible.
- Breaches of this policy and related privacy policies may be subject to disciplinary action as outlined in the Confidentiality Statement (form 900063)
- NHS and its agents are also subject to the fines and penalties set out in PHIPA up to \$50,000 for individuals and \$250,000 for the organization.

Identifying Purposes for the Collection of Personal Health Information

At, or before the time personal health information is collected, NHS will identify the purposes for which personal health information is collected. Permitted purposes are the delivery of direct patient care, the administration of the health care system, research, teaching, statistics, fundraising, and meeting legal and regulatory requirements as described in PHIPA.

- Identifying the purposes for which personal health information is collected at or before the time of collection allows the NHS to determine the information it needs to collect to fulfill these purposes.
- The identified purposes are specified at, or before, the time of collection to the individual from whom the PHI is collected. Depending upon the way in which the information is collected, this can be done verbally or in writing.
- A patient who presents for treatment is also giving implied consent for the use of his or her personal health information for authorized purposes.
- Notices identifying the purposes for the collection of personal health information are readily available to patients. (see Openness for further details.)

- When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless law requires the new purpose, the consent of the individual is required before information can be used for that purpose.
- Persons collecting personal health information will be able to explain to individuals the purposes for which the information is being collected.

Consent for the Collection, Use and Disclosure of Personal Health Information

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal health information, except in certain circumstances.

Note: In certain circumstances, personal health information can be collected, used or disclosed without the knowledge and consent of the individual. Seeking consent from the patient may be impossible or inappropriate, for example when the individual is seriously ill or mentally incapacitated. In these circumstances, consent of the individual's substitute decision maker will be sought, where feasible.

- Consent is required for the collection of PHI and the subsequent use or disclosure of this information.
- NHS will make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.
- Individuals can give consent in many ways. For example:
 - a. A 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 specified uses and/or disclosures.
 - b. Consent may be given verbally or in writing at the time that individuals use a health service.
 - c. Consent may be given verbally when information is collected over the telephone.
- In cases where express consent is required and it is provided verbally, this exchange is documented in the patient's record of personal health information.
- An individual may withdraw consent at any time, subject to legal restrictions and reasonable notice. Withdrawal of the consent will not have a retroactive effect. NHS will inform the individual of the implications of such withdrawal.

Limiting Collection of Personal Health Information

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

- NHS will not collect personal health information indiscriminately. Both the amount and the type of information collected will be limited to that which is necessary to fulfill the purposes identified.
- The requirement that personal health information be collected by fair and lawful means is intended to prevent NHS from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

Limiting Use, Disclosure and Retention of Personal Health Information

Personal health 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.

- If using or disclosing personal health information for a new purpose, NHS will document this purpose. Unless law permits the new purpose, the consent of the individual is required before information can be disclosed or used for that purpose.
- NHS has developed policies and implemented procedures with respect to the retention of health information, which are clearly established in data-sharing agreements and contracts.
- Information that is no longer required will be destroyed or erased after the agreed-upon retention period has been met as per the NHS Retention and Destruction policies.

Ensuring Accuracy of Personal Health Information

NHS will take reasonable steps to ensure that information is as accurate, complete, and up to date as is necessary to minimize the possibility that inappropriate information may be used to make a decision about the individual.

- Limitations on the accuracy and completeness of personal health information disclosed will be clearly set out to the recipient where possible.
- When an individual successfully demonstrates the inaccuracy or incompleteness of personal health information, the NHS will amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information will be transmitted to third parties having access to the information in question.
- When a challenge is not resolved to the satisfaction of the individual, the NHS will record the substance of the unresolved challenge in the form of a letter from the patient stored in the patient's health record. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

Ensuring Safeguards for Personal Health Information (PHI)

Niagara Health System will protect all PHI within its custody and control. NHS considers all PHI to be highly sensitive; thus information protection is paramount and accomplished with security safeguards appropriate to the sensitivity of the PHI.

- Security safeguards are used to protect personal health information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. NHS protects personal health information regardless of the format in which it is held.
- The nature of the safeguards will vary depending on the amount, distribution, format of the information and the method of storage. The methods of protection will include:
 - a. Physical measures, for example, locked filing cabinets and restricted access to offices
 - b. Organizational measures, for example, policies, training, limiting access on a "need-to-know" basis, confidentiality statements, data-sharing agreements;
 - c. Technological measures, for example, the use of passwords, secure computer networks, and audits, use of firewalls.
- NHS will make its employees aware of the importance of maintaining the confidentiality of personal health information. All new NHS employees/agents (e.g., employee, clinician, allied health, volunteer, researcher, student, consultant, or contractor) sign a Confidentiality Statement (form #900063) with the NHS. This safeguard may also be facilitated through contractual provisions.
- NHS has policies and procedures in place pertaining to the disposal or destruction of personal health information, to prevent unauthorized parties from gaining access to the information.

Openness About Personal Health Information Policies & Practices

NHS makes information on its policies and practices available in a variety of ways. For example, NHS may choose to make brochures available, post signs, or provide information online via its public web site.

- A written public statement is made available to the public. This notice:
 - a. provides a general description of NHS information practices
 - b. describes how to contact the NHS Privacy Officer (the designated privacy contact)
 - c. describes how an individual may obtain access to or request correction of a record of personal health information
 - d. describes how an individual may make a complaint to NHS or to the Information and Privacy Commissioner of Ontario.

Individual Access to Own Personal Health Information

Upon request, an individual will be informed of the existence, use, and disclosure of his or her personal health 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.

Note: In certain situations, NHS may not be able to provide access to all the personal health information it holds about an individual. Exceptions to the access requirement will be in accordance with the law. The reasons for denying access will be provided to the individual. Examples may include information that could reasonably be expected to result in a risk of serious harm or the information is subject to legal privilege.

- Upon request, NHS will inform an individual whether or not it holds personal health information about that individual. NHS will seek to indicate the source of this information and will allow the individual access to this information. However, it may choose to make sensitive medical information available through a medical practitioner.
- An individual will be required to provide sufficient information to permit NHS to provide an account of the existence, use, and disclosure of personal health information. The information provided will only be used for this purpose.
- In providing an account of third parties to which it has disclosed personal health information about an individual, NHS will attempt to be as specific as possible.
- NHS will respond to an individual's request within the period specified in the Personal Health Information Protection Act. The NHS may charge the individual a fee for service in accordance with the NHS fee schedule.

Challenging Compliance with NHS Privacy Policies & Practices

An individual will be able to address a challenge concerning compliance with this policy.

- NHS has procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal health information.
- NHS will inform individuals who make inquiries or lodge complaints, of the existence of relevant complaint procedures.
- If individuals have questions or concerns about NHS privacy practices, they may contact the NHS Chief Privacy Officer. Written complaints are to be directed to: Patient Relations Specialist, Ontario Street Site, 155 Ontario Street, St.Catharines, ON L2R 5K3

- If individuals require more information about their privacy rights, or are unable to resolve a problem with the NHS, they may contact the Ontario Information and Privacy Commissioner, 2 Bloor Street East, Suite 1400, Toronto, ON M4W 1A8; call 1-800-387-0073, or email to: info@ipc.on.ca.

4.0 Related Documents

Collection, Use and Disclosure of Personal Health Information P&P
 Appendix A– Decision Tree for Consent
 Appendix B – Consent for Disclosure of PHI/Request for Access to PHI, (Form 900035)
 Patient Request for Opt-Out of Hospital Directory, Family Physician, Religion, Fundraising P&P
 Internal and External Transmission of Health Information by Facsimile P&P
 Patient Substitute Decision Maker Access to and Disclosure of PHI P&P
 Appendix A- Refusal to Access, Correction of Personal Health Record
 Appendix B- Extension Letter to Comply with Access, Disclosure Request
 Patient Substitute Decision Maker Request for Correction to PHI P&P
 NHS Release of Personal Health Information Fee Schedule Policy
 Addressing Confidentiality Security Violations of PCI P&P
 Monitoring System for Patient Care Inquiry PCI Audit Trails P&P
 Confidentiality Statement and PHI P&P
 Form 900063 – Confidentiality Statement
 Missing, Lost or Stolen PHI P&P
 Appendix A - Letters
 Sequestered Records P&P
 Retention, Storage and Destruction of PHI P&P
 Appendix A – NHS Record Destruction – Chart Log
 Appendix B - Certificate of Destruction

5.0 References

Ontario Personal Health Information Protection Act, 2004
 Public Hospitals Act, Reg. 965
 ICES – Institute for Clinical Evaluative Sciences – Privacy Code,
 Protecting Personal Health Information at ICES

Review Dates:

Revision Dates:
