Hospital Privacy Toolkit

Guide to the Ontario Personal Health Information Protection Act

Ontario Hospital Association, Ontario Hospital eHealth Council, Ontario Medical Association, Office of the Information and Privacy Commissioner/Ontario

Publication # 314

September 2004

ISBN 0-88621-310-X

WARNING AND DISCLAIMER

This Toolkit has been prepared by McMillan Binch LLP and IBM Business Consulting Services for the Ontario Hospital Association, for the ownership and use of the Ontario Hospital Association and the Ontario Hospital eHealth Council, the Ontario Medical Association, the Office of the Information and Privacy Commissioner and the Ministry of Health and Long-Term Care, as a general guide to assist hospitals and physicians to meet their obligations under the *Personal Health Information Protection Act, 2004*.

- This Toolkit is designed to assist in complying with the law and meeting the changing expectations of patients and the public.

- The resource materials provided in this Toolkit are for general information purposes only. They should be adapted to the circumstances of each hospital or physician using the Toolkit.

- This Toolkit reflects interpretations and practices regarded as valid when it was published based on available information at that time.

- This Toolkit is not intended, and should not be construed, as legal or professional advice or opinion.

- Hospitals or physicians concerned about the applicability of privacy legislation to their activities are advised to seek legal or professional advice based on their particular circumstances.

- In addition, Ontario's Information and Privacy Commissioner has an important role to play in providing further guidance on how the Personal Health Information Protection Act, 2004 is being applied and interpreted. You should monitor the Commission's website at http://www.ipc.on.ca as well as that of the Ministry of Health and Long-Term Care at http://www.health.gov.on.ca/english/public/updates/archives/hu_03/priv_legislation.html.

This is the first edition of the Toolkit. A second edition may be published in due course. Your feedback on this first edition is appreciated.

ACKNOWLEDGEMENTS

Consultants

This Toolkit was written and produced for the Ontario Hospital Association, the Ontario Medical Association, the Ontario Hospital E-Health Council, the Information and Privacy Commissioner/Ontario and the Ministry of Health and Long-Term Care by the following team drawn from McMillan Binch LLP and IBM Business Consulting Services:

McMillan Binch LLP

Simon Chester

LYDIA WAKULOWSKY
Principal Author

Holly Agnew
Grant Carmichael
Sarah Diamond
Rebecca Huang
Reema Kapoor
Sharon Mitchell-Kamara
Ginevra Saylor

IBM Business Consulting Services

Neil Stuart

Erfa Alani
Nigel Brown
Janice Edgecombe
Lane Ilersich
Marta Yurcan

Steering Committee/Privacy Toolkit Working Group

We wish to acknowledge and thank the members of the Steering Committee and Privacy Toolkit Working Group (PTWG) who contributed to the development of this toolkit:

Steering Committee

Brian Beamish, Director, Policy and Compliance, Information and Privacy Commissioner / Ontario

Elizabeth Carlton, Senior Advisor, Legislation & Policy, Ontario Hospital Association

Susan Crozier (Chair of PTWG), Corporate Chief Privacy Officer, Royal Ottawa Health Care

Nancy Gabor, eHealth Analyst, Ontario Hospital eHealth Council

Debra Grant, Senior Health Privacy Specialist, Information and Privacy Commissioner / Ontario

Barb LeBlanc, Director, Health Policy, Ontario Medical Association

Michele Sanborn, Manager, Health Information Privacy, Ministry of Health and Long-Term Care

Joanne Serraf, Project Manager, Privacy Toolkit, Ontario Hospital Association

Privacy Toolkit Working Group

Meredith Appleby, Privacy Officer, Shared Services West

Elaine Cathcart, Privacy Compliance Manager, Niagara Health System

Jane Dargie, Director, Privacy, Smart Systems for Health Agency

Kate Dewhirst, Legal Counsel, Centre for Addiction and Mental Health

Mary Gavel, Director, Risk Management and Patient Relations, Rouge Valley Health System

Elizabeth Goff, Privacy Officer, St. Joseph's Health Centre (Toronto)

Dr. Ron Heslegrave, Chair, Research Ethics Board, University Health Network and Mount Sinai Hospital

Tiffany Jay, Privacy Manager, University Health Network

Peter Lambert, Manager, Information Security, St. Michael's Hospital

Don Livingstone, Chief Medical Officer, Sunnybrook & Women's College Health Sciences Centre

Roberta MacDonald, Director, Information Systems / Chief Privacy Officer, St. Mary's General Hospital

Sara McRae, Privacy Officer, Lakeridge Health

Sharon Pfaff, Chief Privacy and Information Officer, Chatham-Kent Health Alliance

Ruth Servos, Health Information Technician, Hotel Dieu Health Sciences Hospital, Niagara

Joyce Seto, Director, Information and Information Technology, Cardiac Care Network of Ontario

Sharon vanValkenburg, Director, Information Services, Temiskaming Hospital

Pearl Veenema, Managing Director of Campaigns, University Health Network

E. Jean Wright, Director, Information Systems, North Bay Psychiatric Hospital and North East Mental Health Centre

Ministry of Health and Long-Term Care

The Ontario Hospital Association also wishes to extend its appreciation to legal counsel of the Ministry of Health and Long Term Care for their time and efforts in reviewing the Toolkit:

Legal Counsel

Fannie Dimitriadis, Legal Counsel, Ministry of Health and Long Term Care

Michael Orr, Legal Counsel, Ministry of Health and Long Term Care

Halyna Perun, Legal Counsel, Ministry of Health and Long Term Care

Funding for this Toolkit was provided by the Ontario Hospital Association, the Ontario Hospital E-Health Council, the Ontario Medical Association and the Ministry of Health and Long-Term Care.

Table of Contents

General Privacy Compliance

Contact Person

Consent

Table of Contents

Collection, Use and Disclosure

Accessing Health Records

Table of Contents

Table of Contents

Security – Institutional Safeguards

Sustaining Security

Table of Contents

Research

Fundraising

Managing Contracts and Agents

Oversight

Table of Contents

General Privacy Compliance

Table of Contents

General Privacy Compliance

Using This Toolkit

A toolkit contains the tools needed to get the job done. In this case, the job is to ensure you comply with the Act. Legislation is not easy to read, let alone interpret and apply to your own situation. This Toolkit provides a variety of tools designed to help you understand and apply the new privacy legislation.

To get started, begin by reading:

1

- General Privacy Compliance – for a very general overview of the Act
- Consent – to understand the foundation of privacy compliance
- Security – to understand how to protect personal health information
- Oversight – to learn about the role and powers of the Information and Privacy Commissioner/Ontario

Then proceed to the sections that affect your role:

2

- Contact Person
- Managing Health Information
- Accessing Health Records
- Correcting Health Records
- Dealing With Health Information
- Research
- Fundraising
- Managing Contracts and Agents

Then use the Diagnostic Tool:

3

- to assess your state of privacy compliance

In each section you will find:

Key Points: A high level summary of the section.

General Privacy Compliance

The Rule: A brief summary of the key requirements of the law.

What You Need To Do: A brief summary of the key tasks that you must perform to comply with the law.

What You Should Do: Recommended best practices for you to consider implementing.

Related Sections of the Act: A list of the sections of the Act discussed in the section, should you want to refer directly to the Act for more information.

Checklists, Templates and Tools: Tools to help you perform the tasks.

To support your understanding of the content, there is a **Glossary** and **Index** at the end.

Overview

Starting November 1, 2004, you must comply with the *Personal Health Information Protection Act, 2004*, Ontario's new health information privacy legislation. The Act regulates how you collect, use, retain, transfer, disclose, provide access to and dispose of patients' personal health information.

The Act has a number of purposes:

- to establish rules for the collection, use and disclosure of personal health information that protect the confidentiality of that information and the privacy of individuals, while facilitating the effective provision of health care,
- with a few limited and specific exceptions, to provide individuals with a right to access and correct their personal health information,
- to provide for independent review and resolution of complaints about personal health information, and
- to provide effective remedies for contraventions of the Act.

Application and Scope of the Act

The Act applies to a variety of organizations and individuals within the health care sector. These organizations and individuals are called *health information custodians,* and include hospitals and health care practitioners. The Act also applies to *agents,* who can be either organizations or individuals, and who are authorized to act for or on a health information custodian's behalf. The Act regulates how *health information custodians* and their *agents* may collect, use, retain, transfer, disclose, provide access to and dispose of patients' *personal health information*. See the Glossary for a definition of the italicized terms.

This Toolkit uses the term "you" for the sake of clarity and brevity. The terms "you" and "your" describe the legal obligations of:

- hospitals, who are *health information custodians*, and who have a broad institutional responsibility for privacy compliance,
- physicians, who are *health information custodians* when operating their own private practice within a hospital (i.e., when they rent out office space at a hospital) and who are *agents* when acting for a hospital (i.e., when they treat patients in the hospital and contribute to patients' health records in that regard), and who have individual responsibility for privacy compliance, and
- hospital professional staff members, administrative staff members, students and volunteers, who are *agents* of the hospital, and who also have individual responsibility for privacy compliance.

Each of these organizations and individuals (i.e., you) must make efforts (to the extent reasonable given the circumstances) to fulfil the key tasks described in this Toolkit, and to protect patients' privacy and the confidentiality of their personal health information.

This Toolkit uses the term "patient" for the sake of clarity and brevity. The term "patient" should be read to include all individuals about whom you collect, use and disclose personal health information.

The Ten Privacy Principles

The Act builds upon and codifies many of the existing high standards and protections found in the common law, and various professional codes, policies and guidelines.

General Privacy Compliance

The Act is also based on ten privacy principles, which are derived from the Canadian Standards Association's Model Code for the Protection of Personal Information. Most privacy legislation in the world is based on these ten privacy principles:

Privacy Principle	**Requirement**
Accountability	Designate a contact person to assist you in meeting your privacy obligations, and to deal with any access requests, privacy related inquiries and complaints, and Commissioner investigations
Identifying Purposes	Inform your patients of the purposes for which their personal health information is collected, used and disclosed, unless otherwise exempted by the Act
Consent	Rely on implied consent, where appropriate, or obtain express consent from your patients when collecting, using or disclosing their personal health information, unless otherwise exempted by the Act
Limiting Collection	Limit your collection of personal health information to that which is necessary for the identified purposes or for purposes that the Act permits or requires
Limiting Use and Disclosure	Limit your use and disclosure of personal health information to the identified purposes, unless you obtain further consent or your use or disclosure is permitted or required by law
Accuracy	Take reasonable steps to ensure that your patients' personal health information is as accurate, complete and up-to-date as is necessary for the purposes for which you use or disclose it Tell the person to whom you disclose information of limitations on the accuracy, completeness or up-to-date character of the information
Safeguards	Implement appropriate technical, administrative and physical safeguards to protect your patients' privacy and the confidentiality of their personal health information Ensure your staff are informed of privacy and confidentiality requirements
Openness	Develop and make available a written statement on your information practices (e.g., your collection, use and disclosure of personal health information)
Access	In a timely manner, give your patients access to, and the ability to correct, their personal health records if they meet the requirements of the Act

Privacy Principle	Requirement
Challenging Compliance	Develop simple complaint procedures to allow individuals to challenge your privacy practices

What You Need to Do

To comply with the Act, you must:

- designate a contact person for the purposes of the Act,
- identify the purposes for which you collect, use and disclose personal health information,
- only collect, use or disclose your patients' personal health information if you have your patients' consent to do so or if the Act allows you to do so without consent,
- only collect, use or disclose your patients' personal health information if no other information would serve your purpose,
- only collect, use or disclose that amount of information necessary to serve your purpose and follow reasonable information practices to protect your patients' personal health information against theft, loss and unauthorized access, copying, modification, use, disclosure and disposal,
- take reasonable steps to ensure that your patients' personal health information is as accurate, complete and up-to-date as needed for its use or disclosure,
- establish and maintain appropriate information practices and tell your patients about these practices (note: the rest of this Toolkit will help you develop these information practices),
- develop and make available a written statement on:
  - your information practices (in general terms),
  - your contact person's contact information, and
  - your access, correction, inquiry and complaints procedures,
- develop procedures to:

  - identify when a use or disclosure of personal health information is beyond what is described in the written statement,
  - notify affected patients about such a use or disclosure, and
  - make and keep notes of such a use or disclosure in or linked to the affected patient's personal health record,

- train your staff, volunteers and others acting on your behalf to follow your information practices and your procedures, and
- take reasonable steps to protect personal health information that you transfer to others (for example, including privacy clauses in your contracts with agents).

Checklists, Templates and Tools

- Sample Written Statement of Information Practices
- For guidelines on establishing information practices, see the Security sections.
- For guidelines on providing access to health records, see the Accessing Health Records section.
- For guidelines on making corrections to health records, see the Correcting Health Records section.
- For guidelines on responding to complaints, see the Oversight section.
- For guidelines on managing others, see the Managing Contracts and Agents section.

NOTE TO USER: When you use this Statement, you must ensure that you have included all of your proposed uses and disclosures. If you use or disclose a patient's personal health information, without the patient's consent, in a manner that is not described on the Statement, you must: (a) inform the patient of this as soon as possible unless the patient does not have a right of access to their personal health record, and (b) make and keep a note of the use or disclosure in or linked to the affected patient's personal health record.

SAMPLE WRITTEN STATEMENT OF INFORMATION PRACTICES

Collection of Personal Health Information

We collect personal health information about you directly from you or from the person acting on your behalf. The personal health information that we collect may include, for example, your name, date of birth, address, health history, records of your visits to **[the Hospital]** and the care that you received during those visits. Occasionally, we collect personal health information about you from other sources if we have obtained your consent to do so or if the law permits.

Uses and Disclosures of Personal Health Information

We use and disclose your personal health information to:

- treat and care for you,
- get payment for your treatment and care (from OHIP, WSIB, your private insurer or others),
- plan, administer and manage our internal operations,
- conduct risk management activities,
- conduct quality improvement activities (such as sending patients satisfaction surveys),
- teach,
- conduct research,
- compile statistics,
- fundraise to improve our healthcare services and programs,
- comply with legal and regulatory requirements, and
- fulfil other purposes permitted or required by law.

Your Choices

You may access and correct your personal health records, or withdraw your consent for some of the above uses and disclosures by contacting us (subject to legal exceptions).

Important Information

- We take steps to protect your personal health information from theft, loss and unauthorized access, copying, modification, use, disclosure and disposal.
- We conduct audits and complete investigations to monitor and manage our privacy compliance.
- We take steps to ensure that everyone who performs services for us protect your privacy and only use your personal health information for the purposes you have consented to.

How to Contact Us

Our privacy contact person is ●.

For more information about our privacy protection practices, or to raise a concern you have with our practices, contact us at:

[Address, fax, email, telephone number and website]

You have the right to complain to the Information and Privacy Commissioner/Ontario if you think we have violated your rights. The Commissioner can be reached at:

[Address, fax, email, telephone number and website]

Contact Person

Table of Contents

Contact Person

Contact Person

Key Points

- You must designate a contact person to assist you in meeting your privacy obligations.
- The contact person will be primarily responsible for privacy compliance activities within your facility.
- This means responsibility for ensuring that your facility has:
  - established and maintains appropriate information practices,
  - developed access, correction, inquiry and complaints procedures, and
  - developed and made available a written statement that describes your facility's information practices, your contact person's contact information, and your access, correction, inquiry and complaints procedures.
- The contact person will deal with any access requests, privacy related inquiries and complaints, and Commissioner investigations.

Contact Person

The Rule

You must designate a contact person to:

What You Need To Do

- Designate a contact person.
- Assign responsibility to the contact person to develop procedures to respond to:
  - patients who ask to review their personal health records,
  - patients who ask to correct their personal health records, and

- inquiries or complaints about possible violations of the law.

What You Should Do

The duties listed under heading What You Need To Do are those required by the Act. You may wish to broaden or complement the contact person's duties to include other work aimed at ensuring your overall compliance with the Act.

For example, the contact person could be responsible for:

- making an assessment of the information you collect and how it is used and disclosed,
- conducing privacy impact assessments and privacy audits of information use,
- developing privacy policies, procedures and tools, and
- informing and assisting agents on privacy matters.

Related Sections of the Act

2, 3, 4, 10, 11, 12, 13, 14, 15, 16, 17

Checklists, Templates and Tools

See the Sample Written Statement of Information Practices in the General Privacy Compliance section.

Consent

Table of Contents

Consent

Key Points

- Generally, you need either *express* or *implied* consent before you may collect, use or disclose personal health information. When you collect, use and disclose personal health information for health care purposes, you can usually rely on *implied* consent. If the purpose is something other than health care, you must often obtain *express* consent. There are also specified circumstances where you may collect, use or disclose personal health information *without consent*.

- To be a valid consent, the patient must have the capacity to consent. Where required, you must obtain consent from the patient's substitute decision-maker if the patient does not have the capacity to consent.

- To be a valid consent, the consent must be obtained voluntarily and directly from the patient (or substitute decision-maker), and the consent must be knowledgeable and related to the information in question.

- Patients have the right to refuse, withdraw or place restrictions on their consent, if the purpose for which their personal health information is collected, used or disclosed requires consent.

- The Act has special rules for dealing with children and teenagers.

- The *Mental Health Act* has additional rules on mandatory and permitted disclosures without consent.

Consent

The Rule

Generally, you need either *express* or *implied* consent before you may collect, use or disclose personal health information. When you collect, use and disclose personal health information for health care purposes, you can usually rely on *implied* consent. If the purpose is something other than health care, you must often obtain *express* consent. There are also specified circumstances where you may collect, use or disclose personal health information without consent.

To be a valid consent:

- the patient must have the capacity to consent (for more information on capacity see page 36),
- it must be obtained directly from the patient or someone with legal authority to consent for the patient (called a substitute decision-maker),
- it must be related to the information in question,
- it must be obtained voluntarily (without deception or coercion), and
- it must be knowledgeable, meaning it must be reasonable to believe that the patient understands:
  - why you are collecting, using or disclosing the information, and
  - that the patient has the right to withhold or withdraw consent.

Note: This section relates to consent to the collection, use and disclosure of personal health information, and not to consent to treatment. The Act has not changed the consent to treatment rules.

What You Need To Do

Implied Consent

There are many circumstances where you may rely on consent that can be implied from your patients' behaviour. The following explains implied consent and when you may rely upon it. It also sets out guidelines to ensure you are correctly relying on implied consent.

What is Implied Consent?

Implied consent permits you to conclude from surrounding circumstances that a patient would reasonably agree to the collection, use or disclosure of the patient's personal health information.

Example: If you ask patients for personal health information to open a record and they answer your questions, you can infer their consent to the collection of their information.

When is Implied Consent Acceptable?

You may rely upon your patients' implied consent if you are:

- a health information custodian collecting, using and disclosing personal health information to provide health care,

  Note: A health information custodian who receives a patient's personal health information from the patient, the substitute decision-maker or another health information custodian for the purpose of providing or assisting in providing health care to the patient may assume that it has the patient's implied consent to collect, use and disclose the information for health care purposes, unless the health information custodian is aware that the patient has expressly withheld or withdrawn the consent.

- collecting, using or disclosing names and mailing addresses for fundraising, or

- providing names and location within the hospital to someone representing the patients' religious or other organization. See the discussion on Spiritual Care in the Managing Health Information section.

Guidelines for Relying on Implied Consent

To ensure that your reliance on implied consent is proper:

- give your patients the information they need to understand why you are collecting their information and how you may use or disclose it.
- do so by posting notices or placing brochures in high traffic areas and waiting rooms:
  - describing why you collect, use and disclose personal health information, and
  - informing patients that they may withhold or withdraw their consent and providing information on how they can do so.
- if you have done this, and your patients have not withheld or withdrawn their consent, you may rely on your patients' implied consent.

Remember: Consent may never be implied if patients specifically state that their personal health information may not be collected, used or disclosed.

See page 11 for a sample notice.

Express Consent

The following explains express consent and when it is required. It also sets out guidelines for obtaining express consent.

What Is Express Consent?

Express consent is obtained when patients explicitly agree to the collection, use and disclosure of their personal health information.

Express consent can be given in writing, orally, by telephone or electronically.

When Is Express Consent Required?

You must get your patients' express consent if you are:

- disclosing personal health information to someone other than a health information custodian.

  Example: You must get express consent if you are disclosing personal health information to an employer or insurance provider.

- disclosing personal health information to another health information custodian for a purpose other than providing or assisting in providing health care.

  Example: You must get express consent if you are disclosing personal health information to another health information custodian for the purpose of research (unless certain conditions and restrictions are met). See the Research section for additional guidance.

  Example: You must get express consent if you are disclosing personal health information to another hospital to establish common patterns in the use of a particular drug or therapy.

- collecting, using or disclosing personal information (other than names and mailing addresses) for fundraising.

Guidelines for Obtaining Express Consent

When obtaining express consent:

- tell your patients the specific reasons why you are collecting their information, how you will use their information, and under what circumstances you may disclose their information to others,

- get to the point and explain why you are asking for consent in clear everyday language,

- although you must tell your patients enough for them to give knowledgeable consent, do not overwhelm them with unnecessary medical or overly technical information,

- create forms with clear explanations (when obtaining written consent),

- only use and disclose personal health information for the purposes for which the patient consented or for purposes permitted without consent under the Act.

- fully document oral consent and how you got it, and
- tell your patients that they can put conditions on or withdraw their express consent any time.

Remember: Although express consent is best from a risk management perspective, it is not always required.

Withdrawal of Consent

Patients may withdraw their consent at any time.

Patients who want to withdraw their consent must notify you that they no longer consent to your collection, use and disclosure of their personal health information.

A patient's withdrawal has no effect on information you collected, used or disclosed before the patient withdrew consent, but has effect from the time it is received.

A substitute decision-maker who consented on a patient's behalf may also withdraw that consent at any time by notifying you.

If the withdrawal of consent will compromise patient care, be sure to discuss the effect of the withdrawal with the patient and carefully document the withdrawal and these discussions in the patient's health record.

Conditional Consent

Patients may place restrictions on their consent. For example, a patient may want you to share information with only a specific organization for a specific purpose.

Such a restriction affects only collections, uses and disclosures that require consent or that are subject to the express instruction ("lock box") provisions. See the Managing Health Information section for additional information on "lock boxes". Also, such a restriction cannot stop you from recording information as required by law, or established professional standards or institutional practice.

When Consent Is Not Required

There are situations where patient consent to the collection, use or disclosure of personal health information is not required.

Examples of these situations are described below.

Collection

You do not need your patients' consent to collect their personal health information if you need the information to treat the patient, you can reasonably rely on the information as accurate and there is no time to obtain consent.

You may *indirectly* collect personal health information without consent if:

- the Commissioner specifically authorizes the collection,
- you collect the information from a person who is permitted or required by law to disclose it to you, or
- you are legally permitted or required to collect it indirectly.

Note: Collecting information "indirectly" means collecting it from a source other than the patient or substitute decision-maker.

Use

You may use personal health information you collect with your patients' consent for the purpose for which you gathered it. Where you have collected personal health information with implied consent, you may use it for all purposes for which it is reasonable to imply consent (see discussion above on implied consent).

Consent is not required to use the information to:

- comply with a legal requirement,
- plan, deliver or monitor health-related programs that you provide,
- manage risk and errors, improve the quality of service or maintain programs,
- educate those working with your patients so they can care for your patients,

  Example: During rounds with your students; however, you need consent to disclose personal health information at grand rounds held in other hospitals.

- dispose of or alter information to ensure that others cannot link the information to a specific individual,
- seek consent to additional collections, uses and disclosures when only patients' names and contact information are used,

- participate in legal or administrative proceedings in which you are involved, or
- collect payment for health care services you provided.

You may also use information for research if certain conditions and restrictions are met (for more information, see the Research section).

Note: When you provide personal health information to your agents, you are "using" the information. This use is not considered a "disclosure" under the Act.

Disclosure

You do not need consent to disclose personal health information to the following people or organizations:

- other health care practitioners or groups of health care practitioners,
- community service providers (defined in the *Long-Term Care Act*),
- community care access corporations,
- public or private hospitals,
- psychiatric facilities,
- independent health facilities,
- homes for the aged, rest homes, nursing homes, care homes,
- pharmacies,
- laboratories,
- ambulance services,
- homes for special care,
- centres, programs and services for community health or mental health whose primary purposes are providing health care,

so long as:

- the information is reasonably necessary to provide health care,
- you cannot get consent when needed, and
- the patient has not specifically told you not to disclose information in certain circumstances.

- a regulated health profession college for the purpose of administration or enforcement of the *Drug and Pharmacies Regulation Act*, the *Regulated Health Professions Act* or an Act named in Schedule 1 to that Act,
- the Ontario College of Social Workers and Social Service Workers for the purpose of administration or enforcement of the *Social Work and Social Service Work Act*,
- the Public Guardian and Trustee, the Children's Lawyer, a children's aid society, a Residential Placement Advisory Committee established under the *Child and Family Services Act* or the Registrar of Adoption Information appointed under that Act so that they can carry out their statutory functions,
- the Archives of Ontario or, in certain limited circumstances, a prescribed person whose functions include collecting and preserving information (when the information is disclosed for that purpose),
- someone auditing or reviewing an accreditation or accreditation application related to health care provision - but the record must not be removed from your premises,
- a researcher following the guidelines in the Research section,
- the Chief Medical Officer of Health or a Medical Officer of Health for purposes set out in the *Health Protection and Promotion Act*,
- a public health authority similar to the Medical Officer of Health established by Canadian federal, provincial or territorial statute so long as information is disclosed for purposes similar to those in the *Health Protection and Promotion Act*,
- the Minister on request to monitor or verify public health fund payments,
- a body created under provincial government regulations that is analyzing or compiling statistics to manage, evaluate or monitor the resource allocation or planning for the health system and related service delivery (so long as that person has appropriate practices and procedures in place to protect patient privacy), except information concerning personal counselling or other information the regulations may exclude, and
- the head of penal (or similar) institution where the patient is being detained in order to arrange treatment or make a decision regarding where the patient should be placed.

Consent

You do not need your patients' consent to disclose their personal health information if:

- you must do so to contact a relative, friend or potential substitute decision-maker of a patient who is injured, incapacitated or ill and unable to give consent personally,
- you are disclosing information you collected to a person listed in the regulations who operates a registry intended to facilitate or improve health care provision or administer the storage or donation of body parts, organs or substances like blood or plasma,
- you are permitted or required by law to provide the information,
- the Minister or other health information custodian needs the information to decide whether to fund or pay a hospital or physician for health care provided,
- the information is needed to determine eligibility for health care or other governmental benefits,
- you reasonably believe the information is needed to prevent serious bodily harm or reduce a significant risk of it happening to any person,
- you disclose personal health information to a potential purchaser of your practice to assess and evaluate your operations, and the potential purchaser agrees in writing to keep the information confidential and secure and keep the information no longer than necessary to reach a conclusion,
- a health data institute that the Minister has approved will use the information to analyze how well the system and related service delivery works, and
- you are doing so for the purpose of a proceeding or contemplated proceeding in which you or your agent (or former agent) is a party or witness, if the information is relevant to the proceeding.

You may disclose patient's personal health information to a person outside Ontario if:

- you have consent or the Act allows you to do so,
- the person receiving the information performs functions comparable to the functions performed by a person within Ontario to whom the Act permits disclosure,
- you must disclose the information for health care purposes (unless the patient has expressly instructed you not to make the disclosure), or

- the disclosure is reasonably necessary for payment of health care purposes.

Psychiatric Facilities

In addition to the disclosures permitted under the Act, the *Mental Health Act* permits the officer in charge of a psychiatric facility to collect, use or disclose personal health information with or without consent to:

- assess, observe, examine or detain the patient in accordance with the *Mental Health Act*, and
- comply with Part 21 of the Criminal Code (Mental Disorder) or an order under that part.

The officer in charge of a psychiatric facility may also disclose a personal health record:

- for proceedings before the Consent and Capacity Board at the request of a party to the proceeding,
- to a physician who is considering, has or is renewing a community treatment order or who has been appointed to supervise and manage the community treatment order,
- to an individual named in the community treatment plan as providing treatment, upon receiving written request of the physician or other named person,
- to a person providing advocacy services in prescribed circumstances,
- to the Public Guardian and Trustee to enable investigations, and

  Note: You must disclose personal health information to the Public Guardian and Trustee where you have a concern about adverse effects occurring to a mentally incapable individual, such as elder abuse. The Public Guardian and Trustee may access the patient's health record for the purpose of investigating the allegation.

- pursuant to a summons, unless the attending physician feels that such disclosure may result in harm to the patient or a third party, in which case, a court or other body may authorize the disclosure.

Disclosure is also permitted for:

- consultation among health care members named in a community treatment order, or
- consultation between a physician and regulated health care professionals, social workers or others where a physician is considering issuing or renewing a community treatment order.

If you have used a *Mental Health Act* Form 14 in the past to get patient consent, you should:

- ensure that the previously obtained consent meets the requirements of the Act before you continue to rely on it, and
- on a going-forward basis, get consent as set out in this Toolkit, unless your patient's situation falls under the *Mental Health Act* exceptions or other exceptions to consent as set out in his Toolkit.

For more information, refer to the *Mental Health Act*.

Patient Capacity

To be capable of consenting, a patient must be able to understand:

- the information needed to make a decision on whether or not the patient should consent to the collection, use or disclosure of personal health information, and
- the consequences of giving, withholding or withdrawing consent.

A patient's ability to consent may change from time to time. For example, a patient's ability to consent may vary depending upon the patient's condition and the type of information involved. You must consider the patient's capacity every time you seek consent.

You may presume a patient is capable of consenting unless you have reason to believe otherwise. For instance, if a patient says or does nothing to make you doubt the patient's capacity when you are asking for consent, you may rely on the consent (whether you see them in person or speak to them on the telephone).

If you determine that the patient does not have the capacity to consent and the patient has not applied for a review of your determination to the Consent and

Capacity Board, you should get the patient's substitute decision-maker's consent instead. If a substitute decision-maker is acting on the patient's behalf for matters related to treatment, personal care service or admission to a care facility (under the *Health Care Consent Act, 1996*), that person would also consent to the collection, use or disclosure of the patient's personal health information if the information is related to the treatment, personal care service or admission to a care facility.

When a patient is not capable of providing consent you may get consent (ranked in order as listed) from the patient's:

- guardian (if the guardian has the authority to make such decisions),
- attorney for personal care or attorney for property (if the attorney has the authority to make such decisions),
- representative (appointed by the Consent and Capacity Board under the *Health Care Consent Act, 1996* if the representative has the authority to give the consent),
- spouse or partner,
- child, custodial parent, or children's aid society or other person legally entitled to give or withhold consent in place of a parent (**Note:** where this is the situation, the child's parent cannot consent on behalf of the child),
- parent with access rights,
- brother or sister, and
- any other relative (related by blood, marriage or adoption).

If the patient has died, you can get consent from the patient's estate trustee or someone who is in charge of administering the patient's estate.

To consent for a patient, the person must be:

- included in the list above,
- available and capable of consenting,
- at least 16 years old or the patient's parent,
- willing to assume responsibility for giving or refusing consent,

- free of any court order or separation agreement prohibiting them from having access to or consenting for the patient, and
- the highest ranked person on the list of potential substitute decision-makers who is available and capable of consenting.

If a patient is not capable of consenting and you cannot find anyone capable of consenting on their behalf and willing to take on this role, contact the Public Guardian and Trustee who can consent for the patient.

The Public Guardian and Trustee can also give consent if two or more equally high-ranking substitute decision-makers disagree about whether to consent. The Public Guardian and Trustee breaks the deadlock.

Children and Teenagers

Children of any age are presumed to have the capacity to consent to the collection, use and disclosure of their personal health information. Do not presume capacity if it is not reasonable to do so in the circumstances.

For children under 16, a parent or other lawful guardian may consent to the collection, use or disclosure of personal health information even if the child has capacity, unless the information relates to:

- treatment within the meaning of the *Health Care Consent Act, 1996* about which the child has made his or her own decision, or
- counselling in which the child has participated on his or her own under the *Child and Family Services Act*.

When you need consent for the collection, use or disclosure of information about a child less than 16, you may either obtain it from that child, if capable, or the parent or other lawful guardian (but not the access parent, unless such a parent has been lawfully authorized in place of the custodial parent to make information decisions). If there is a conflict between the child and the parent, the capable child's decision prevails with respect to the consent.

Dealing With Substitute Decision-Makers

When treating children and adults who cannot understand what it means to give or withhold consent to the collection, use or disclosure of personal health information, you must ask for a substitute decision-maker's consent, where it is required.

When substitute decision-makers are involved:

- The substitute decision-maker may be the patient's legal guardian, attorney for personal care, spouse or partner, parent, child, sibling or other relative.
- A substitute decision-maker should consent only if:
  - the patient is incapable or the patient is capable and is 16 or older but has authorized in writing a substitute decision-maker to consent on the patient's behalf,
  - the substitute decision-maker can consent, and
  - the substitute decision-maker is not prohibited by a court order or separation agreement from having access to the patient.
- Always make sure substitute decision-makers understand and are willing to assume consent responsibilities by discussing the responsibilities with them.
- Substitute decision-makers must consider the patient's wishes and beliefs, the benefits to the patient, why the information will be collected, used or disclosed, and whether collecting the information is necessary.

If you do not believe that a substitute decision-maker properly considered the required factors, you may apply to the Consent and Capacity Board (created under the *Health Care Consent Act*) to determine whether the substitute decision-maker met the requirements.

Related Sections of the Act

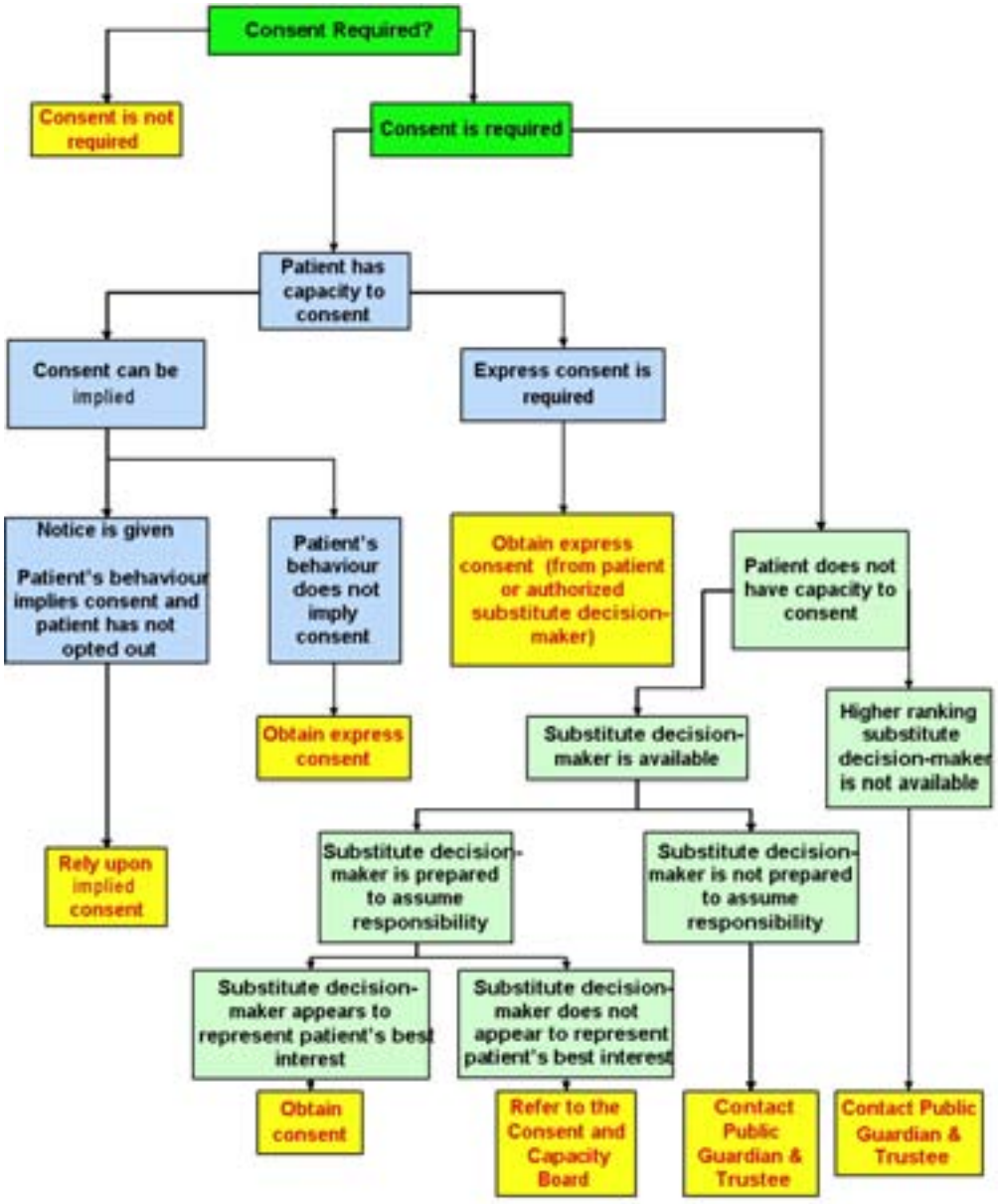
3, 5, 6, 9, 16(2), 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 32, 33, 36, 37, 38, 39, 42, 43, 44, 45, 46, 47

Checklists, Templates and Tools

- Decision Tree for Consent
- Consent Form
- Withdrawal of Consent Form

Consent

DECISION TREE FOR CONSENT



NOTE TO USER: This Sample Consent Form provides a sample list of purposes for the collection, use and disclosure of personal health information where *express consent* is required under the Act. You should consider whether your intended purpose for the collection, use and disclosure of personal health information requires *express consent* and amend this form to include all such purposes. If you choose to rely on express oral consent, no such form is needed.

SAMPLE CONSENT FORM

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

I, _____, have reviewed the **[Hospital]**'s written statement concerning the collection, use and disclosure of personal health information.

I understand that the **[Hospital]** is seeking my consent for it to collect, use and/or disclose my personal health information from me or from the person acting on my behalf to

- ❑ teach outside the **[Hospital]**.
- ❑ fundraise for the **[Hospital]**'s charitable activities, using more than my name and mailing address,
- ❑ _____, and
- ❑ _____.

I understand that the **[Hospital]** will only collect, use and disclose my personal health information with my consent **[as set out in its written statement/privacy policy]** unless a particular collection, use or disclosure is permitted or required by law without my consent.

I also understand that I can refuse to sign this consent form. I can also withdraw my consent any time by writing to ●.

I hereby authorize **[Hospital]** to collect, use and disclose my personal health information for the purposes that I have checked-off above.

Name: _____

Address: _____

Signature: _____ Date: _____

FOR INTERNAL OFFICE USE ONLY
Patient ID No. _____

SAMPLE WITHDRAWAL OF CONSENT FORM

Withdrawal of Consent

I, _____, wish to withdraw my consent to any further use or disclosure by [Hospital/Physician name] of my personal health information for: (Please check all that apply)

- ☐ Teaching outside the **[Hospital]**.
- ☐ Fundraising, using more than my name and mailing address.
- ☐ _____, and
- ☐ _____

I wish to place the following conditions on any further use or disclosure of my personal health information:

_____

_____

_____

(Please specify conditions)

This withdrawal of consent does not have retroactive effect nor does it affect the uses and disclosures of personal health information collected by **[Hospital/Physician Name]** where the uses and disclosures are permitted or required by law without consent.

Name: _____

Address: _____

Signature: _____ Date: _____

Collection, Use and Disclosure

Table of Contents

Collection, Use and Disclosure

Key Points

- You must only collect, use and disclose your patients' personal health information in compliance with the law.
- This means you must not collect, use or disclose patients' personal health information unless:
  - you have the patients' consent and your collection, use or disclosure is, to the best of your knowledge, necessary for a lawful purpose, or
  - the collection, use or disclosure is permitted or required by the Act.
- You must identify the purposes for which you collect your patients' personal health information in your written statement.
- You must not collect, use or disclose more personal health information than is reasonably necessary to meet your purposes. This limitation does not apply to collections, uses or disclosures required by law.
- You must not collect, use or disclose personal health information if other information will serve your purposes.
- If you collect personal health information in contravention of the Act, you must not use or disclose it unless you are required by law to do so.
- You must not charge patients a fee for collecting or using their personal health information, unless permitted to do so under the Act.
- When disclosing personal health information, you must not charge fees that exceed the prescribed amount or, if no amount is prescribed, a reasonable cost recovery charge.

Collection, Use and Disclosure

The Rule

Generally, you will collect, use and disclose personal health information for health care purposes. However, you might also collect, use and disclose personal health information for other purposes. These other purposes might include financial reimbursement, education, research, statistics, public health regulation compliance, litigation, quality improvement and other purposes permitted or required by law.

The law generally says that you need either express or implied consent when you collect, use or disclose personal health information. When you collect, use and disclose personal health information for health care purposes, you can usually rely on *implied consent*. If the purpose is something other than health care, you must often obtain *express consent*. There are also specified circumstances where you may collect, use or disclose personal health information *without consent*.

See the Consent section for more information and guidelines on consent.

In addition, unless you can rely on an exemption under the law, you must:

- identify the purposes for which you collect, use and disclose your patients' personal health information (this would be done in your written statement – see the General Privacy Compliance section for guidelines on the written statement),
- limit your collection, use and disclosure to information that is reasonably necessary to serve your purposes, and
- not collect, use and disclose personal health information if other information will serve your purposes.

Collection

What You Need To Do

- You must only collect your patients' personal health information in compliance with the law.

- You must identify the purposes for which you collect your patients' personal health information in your written statement.

* See the Consent section for guidelines on when you may collect personal health information with implied or express consent or without consent.

* See the General Privacy Compliance section for guidelines on the written statement.

What You Should Do

- Define scopes of practice and job responsibilities for health care professionals and staff to identify who requires personal health information, what information they require, and for which purpose.
- Inform health care professionals and staff:
  - about who collects what personal health information (to limit duplication of collection),
  - about the consent requirements for collection,
  - about restricting the collection of personal health information to the purposes for which you have consent or which are permitted or required by law, and
  - about restricting the collection of personal health information to the information that is required.
- Regularly review your collection practices to ensure compliance with the Act.

Use

What You Need To Do

- You must only use your patients' personal health information in compliance with the law.
- You must identify the purposes for which you use personal health information in your written statement.

* See the Consent section for guidelines on when you may use personal health information with implied or express consent or without consent.

* See the General Privacy Compliance section for guidelines on the written statement.

What You Should Do

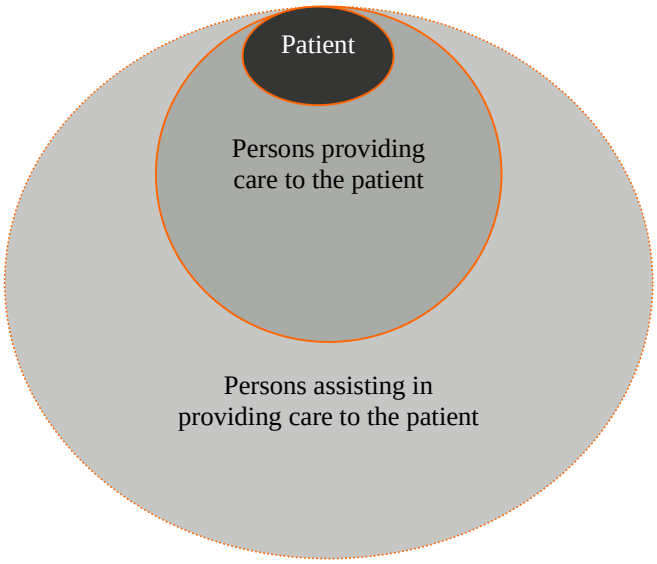
- Develop policies on who is authorized to use your patients' personal health information and for which purpose.
- Inform health care professionals and staff about:
  - the purposes for which they may use personal health information,
  - the consent requirements for use,
  - when other information will suffice, and
  - the need to restrict the use of personal health information to the purposes for which you have consent or which are permitted or required by the law.
- Develop policies to address consent requirements.
- Caution your agents with whom you share personal health information for non-health care purposes that:
  - the information is only to be used for the purposes for which it was shared, unless the use is permitted or required by the Act, and
  - the information must be returned or disposed of securely once that purpose has been fulfilled.
- Consider whether de-identified information can be used to serve the same purpose (e.g., for research or quality of care purposes).

Preventing Unauthorized Use by Authorized Users

- Ensure staff members have clearly defined responsibilities related to the use of personal health information.

- Develop guidelines and inform internal agents (e.g., staff) that personal health information must only be accessed for authorized uses (for example, staff cannot look up information about family members, friends etc.).
- Track and audit staff access to personal health information.
- Ensure external agents (e.g., suppliers) who use personal health information can be held accountable and have an enforceable duty to keep the information secure.
- Where reasonable, use non-disclosure agreements that require:
  - limiting the use of personal health information to the purpose for which it was provided,
  - de-identifying personal health information, where practical,
  - putting in place physical, administrative and technological security measures to reduce the risk of unauthorized use and disclosure, and
  - destroying or having a designated person destroy personal health information after the purpose has been met, if permitted by law.

Use of Personal Health Information by the Circle of Care



"**Circle of care**" is not defined in the Act but refers to those in the health care team who are actually involved in the care or treatment of a particular patient. The term "circle of care" describes those:

- health care practitioners and groups of health care practitioners,
- public and private hospitals,
- pharmacies,
- laboratories,
- ambulance services,
- community care access corporations,
- community service providers (defined in the *Long-Term Care Act*),
- psychiatric facilities,
- independent health facilities,
- homes for the aged, rest homes, nursing homes, care homes and homes for special care, and
- community health or mental health centres, programs and services whose primary purposes are providing health care,

who provide health care or assist in providing health care to a particular patient.

Members of a particular patient's "circle of care" can provide health care to the patient, confidently assuming that they have consent to collect, use and disclose the patient's personal health information for that care, unless they know that the patient has expressly withheld or withdrawn consent.

For example:

- In a hospital, the circle of care includes the attending physician and the health care team (e.g., residents, nurses, technicians and support staff assigned to the patient) who provide care or assist in providing care to the patient.

- But in a hospital, the circle of care does not include health care practitioners who do not provide care to the patient.

- In a physician's office, the circle of care includes the physician and any physicians who provide on-call services, the nurse and support staff who provide care or assist in providing care to the patient.

- But in a physician's office, the circle of care does not include the other physicians in a group practice who do not provide care to the patient.

Videotaping, Audiotaping and Photographing Personal Health Information

You may videotape, audiotape or photograph personal health information for patient care and medical educational purposes.

Patient Care

To assist in the provision of care you may videotape, audiotape or photograph a procedure. When you do so, remember that the tape or photograph becomes part of the patient's health record and is to be treated in the same manner as other personal health information.

When obtaining patient consent (whether express or implied), remember the heightened sensitivity of the taped or photographed information from the patient's perspective. Best practices dictate that you obtain express consent to the collection, use and disclosure of personal health information in this manner; however, as with other circumstances, you may rely on implied consent. Once the tape or photograph is made, make sure you have appropriate safeguards in place to protect its confidentiality (See the Safeguards section for guidelines).

Medical Education

Procedures may be videotaped, audiotaped or photographed for general educational purposes. If you plan to use the tape or photograph to educate your agents to provide health care, you do not need to obtain your patients' consent. However, it may be prudent for you to obtain express consent from your patients, especially if you are facing them with a camera.

When obtaining consent, tell patients:

- the specific personal health information that you intend to record,

- the exact educational purpose for which the information will be used (for instance, a clinical demonstration or a case study),
- the intended audience (for example, undergraduate students or clinical practice rounds, meetings or video- or teleconferences),
- that they can withhold or withdraw their consent at any time, and
- that they will not benefit or suffer from their decision to withhold or withdraw consent.

You should also ensure that the necessary safeguards are in place to protect the confidentiality of the videotapes, audiotapes and photographs (see the Safeguards section for guidelines).

You should de-identify information about a patient when you disclose patient case details to health care practitioners for formal educational programs, where possible.

If you disclose personal health information for educational purposes to health care practitioners or students who are not agents of your facility, you must obtain the affected patients' express consent. For example, if you disclose personal health information at grand rounds of another hospital, you must obtain express consent. If you are doing rounds in your own hospital, but outside guests (i.e., non-agents) have been invited to the rounds, you must obtain express consent.

Disclosure

What You Need To Do

- You must only disclose your patients' personal health information in compliance with the law.
- You must identify the purposes for which you disclose personal health information in your written statement.

* See the Consent section for guidelines on when you may disclose personal health information with implied or express consent or without consent.

* See the General Privacy Compliance section for guidelines on the written statement.

What You Should Do

When assessing third party disclosure requests:

- Inform all staff that disclosure requests must be evaluated on the basis of the type, purpose and requesting party, and whether other information can serve the purpose for which disclosure of personal health information is sought.
- Inform all staff on the consent requirements for disclosure, including when personal health information can be disclosed without consent.
- Develop a policy that incorporates the following steps:
  - verifying the identity of the requesting party,
  - seeking assistance from an appropriate resource, such as the contact person, legal counsel or a mental health practitioner if a request is unusual or if there is uncertainty about whether disclosure should be made,
  - assessing whether further consultation is necessary and whether further legal processes may apply if the disclosure is required by law,
  - including written consent in the patient's personal health record, or documenting the date of consent, and date of disclosure in the patient's personal health record, where express consent is necessary,

- providing only a copy of the personal health record if a personal health record is requested,

- designating a resource (e.g., the contact person) to be responsible for:

  - understanding the rules governing disclosure of personal health information, and

  - recognizing when you need to consult with others.

Situations Involving Disclosure

Disclosure to Family Members or Friends

If you are asked to disclose personal health information about a patient by the patient's family member or friend you can only disclose the personal health information with the patient's or substitute decision-maker's consent.

You must:

- verify that the patient or substitute decision-maker has consented to the disclosure of the personal health information to the patient's family members or friends,

- understand the purpose for which the personal health information is being requested, and

- only disclose personal health information for which you have consent to disclose and that serves the purpose for which the disclosure is requested.

You should:

- confirm the family member's or friend's identity, and

- document the date of the request and the disclosure of the personal health information in the patient's personal health record.

You may disclose the following information if you provide the patient with an opportunity to object at the first reasonable opportunity after admission to your hospital and the patient does not do so:

- whether or not the individual is a patient of your hospital,

- the patient's general health status (e.g. critical, poor, fair, stable or satisfactory), and

- the patient's location in your hospital.

If the Patient is Deceased

You may disclose personal health information about any patients who die, or who you reasonably believe have died, to:

- identify a patient,
- notify another person that a patient died and how they died, and
- provide the immediate family with information they believe they need to make decisions about their own health care.

You can obtain consent from a deceased patient's estate trustee to collect, use or disclose any personal health information of a deceased patient where consent is required. In this instance, you should verify the identity of the estate trustee by reviewing the notarized "Certificate of Appointment of Estate Trustee with a Will" or "Certificate of Appointment of Estate Trustee without a Will". You should also keep a copy of this certificate of appointment.

If the deceased patient does not have an estate trustee, you can obtain consent from the person who has assumed this responsibility, if it is reasonable for you to rely on the accuracy of the assertion made by that person, regarding their identity.

In-Patient Transfer

The physician at the sending facility and the physician at the receiving facility are jointly responsible for determining what personal health information should be provided when a patient is transferred from one facility to another. Where you cannot obtain specific instructions from the physician or if you are facing an emergency transfer, you should send a copy of the patient's complete personal health record. You should also ensure that the records are sealed in a container and securely transferred. You should not transfer records if a patient has withdrawn consent.

Volunteers

Your volunteers are considered to be your agents. Because volunteers may learn personal health information about patients, you should provide volunteers with training on the protection of patient privacy. You should also have them sign a confidentiality agreement.

Spiritual Care

In hospitals, spiritual or religious issues often arise. You may:

- collect information about your patients' religious or other organizational affiliations but only with their consent, and
- rely on your patients' implied consent if they provide you with information about their religious or other organizational affiliations, to provide or disclose the patient's name and location in the hospital to a representative of the religious or other organizational body specified by the individual,

but only if the patient has been given the opportunity to opt out of this disclosure and has not done so.

If a hospital provides a religious program (such as a chaplain visiting program) to its patients, the staff member (e.g., the chaplain) who delivers the program may use personal health information about the hospital's patients for the purposes of this program, without first obtaining consent.

Disclosure to the Media

The following practices may help you to address requests for information from the media:

- Direct all media requests for patients' personal health information to your CEO or designate (e.g., your Communications Department).
- Ensure members of the media identify themselves, the organizations they represent, and the specific personal health information they request.
- Prohibit the media from taking photographs without consent and otherwise invading patient privacy.
- Escort members of the media (through a staff member) when they are on your premises, and take steps to ensure they do not have access to personal health information, except with patient consent.
- Clear media requests to visit your premises in advance through the CEO or designate to ensure proper arrangements are made.
- Ensure members of the media wear a visitor's badge when on your premises.
- Ensure patients sign consent forms for any media photographs or disclosure of other personal health information.

- Develop a procedure on how to handle media inquiries outside of your regular business hours.

Lock Boxes

"**Lock box**" is not defined in the Act but it is an important concept about patients' ability to control their own personal health information.

Patients have the right to expressly instruct you not to use specified personal health information for health care purposes. Patients can also expressly instruct you not to disclose specified personal health information to others (even to others within their circle of care).

The term "lock box" describes the limits that patients can place on the use and disclosure of their personal health information.

If you disclose personal health information about a patient to another member of the patient's circle of care, but the patient has restricted (or locked) you from disclosing all of the personal health information that you consider reasonably necessary to provide health care, you must flag for the recipient that the information is incomplete because the patient has "locked" it.

If you receive this kind of notice from another member of your patient's circle of care, you may choose to discuss the fact that information is restricted with the patient. For example, you can talk about the impact of the restriction on treatment. But you must obtain the patient's express consent before accessing and using the locked information.

Note, however, that a patient cannot restrict a use or disclosure that the Act otherwise permits or requires. The Act trumps the lock box. For example, you may disclose locked personal health information where, in your professional opinion, you need to disclose the information to prevent serious bodily harm or to reduce a significant risk of it happening to any person.

The lock box provisions take effect on November 1, 2004 when the Act comes into force. However, under the Act, hospitals are not required to comply until November 1, 2005.

You should use this time period to develop and implement appropriate procedures to deal with lock box instructions.

Disclosure Tables

The issue of disclosure is complex. The following tables provide a pictorial representation of the most common examples of disclosures to help you determine when disclosure must or can be made. See the Consent section for further information on disclosures that must or can be made without consent.

Mandatory Disclosure

The Act specifically permits the disclosure of personal health information for a number of purposes as required by other statutes. Consent is not required for these specific purposes. For example, you are required to provide the following information:

To whom disclosure must be made	**What information must be disclosed**	**Authority**
Aviation Medical Advisor (note this is a mandatory disclosure for a physician not for a hospital)	Information about flight crew members, air traffic controllers or other aviation licence holders who have a condition that may impact their ability to perform their job in a safe manner	*Aeronautics Act*
Chief Medical Officer of Health or Medical Officer of Health	Information to diagnose, investigate, prevent, treat or contain communicable diseases	*Health Protection and Promotion Act* *Personal Health Information Protection Act*
Chief Medical Officer of Health or Medical Officer of Health or a physician designated by the Chief Medical Officer of Health	Information to diagnose, investigate, prevent, treat or contain SARS	*Public Hospitals Act*
Children's Aid Society	Information about a child in need of protection (e.g., abuse or neglect)	*Child and Family Services Act*

To whom disclosure must be made	What information must be disclosed	Authority
College of a regulated health care professional	Where there are reasonable grounds to believe a health care professional has sexually abused a patient, details of 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 You must also include your name as the individual filing the report.	*Regulated Health Professions Act*
College of a regulated health care professional	A written report, within 30 days, regarding revocation, suspension, termination or dissolution of a health care professionals' privileges, employment or practice for reasons of professional misconduct, incapacity or incompetence	*Regulated Health Professions Act*
College of Physicians and Surgeons of Ontario	Information about the care or treatment of a patient by the physician under investigation	*Public Hospitals Act* Notice must be given to the Chief of Staff and the administrator of the hospital
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 Information requested for the purpose of an investigation	*Coroners Act*
Minister of Health and Long-Term Care	Information for data collection, organization and analysis	*Public Hospitals Act*
Ontario Health Insurance Plan	Information about the funding of patient services	*Public Hospitals Act*

To whom disclosure must be made	What information must be disclosed	Authority
Order, warrant, writ, summons or other process issued by an Ontario court	Information outlined on the warrant, summons, etc.	*Personal Health Information Protection Act*
Physician assessor appointed by the Ministry of Health and Long-Term Care	Information to evaluate applications to the Underserviced Area Program	*Public Hospitals Act*
Registrar General	Births and deaths	*Vital Statistics Act*
Registrar of Motor Vehicles (note this is a mandatory disclosure for a physician not for a hospital)	Name, address and condition of a person who has a condition that may make it unsafe for them to drive	*Highway Traffic Act*
Subpoena issued by an Ontario court	Information outlined in the subpoena	*Personal Health Information Protection Act*
Trillium Gift of Life Network	For tissue donations or transplants purposes, notice of the fact that a patient died or is expected to die imminently (not in force yet)	*Trillium Gift of Life Network Act* Consent must be decided jointly with the Network to determine the need to contact the patient or substitute decision-maker
Workplace Safety and Insurance Board	Information the Board requires about a patient receiving benefits under the *Workplace Safety and Insurance Act*	*Workplace Safety and Insurance Act*

The following tables outline examples of where personal health information may be disclosed. See also the Consent section for additional information on permitted disclosures.

Disclosure for Health Related Programs and Legislation

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Ambulance services operator or delivery agent or the Minister	Administration/enforcement of the *Ambulance Act*	No	*Ambulance Act*
Cancer Care Ontario, Canadian Institute for Health Information, Institute for Clinical Evaluative Sciences or Pediatric Oncology Group of Ontario	To analyze or compile statistical information	No	*Personal Health Information Protection Act* regulations
Chief Medical Officer of Health, Medical Officer of Health or a physician designated by the Chief Medical Officer of Health	To report communicable diseases	No	*Health Protection and Promotion Act*
College of Pharmacists Investigator	Administration/enforcement of the *Drug Interchangeability and Dispensing Fee Act*	No	*Drug Interchangeability and Dispensing Fee Act*
College under the RHPA, or *Social Work and Social Service Act*, or Board of Regents under the *Drugless Practitioners Act*	Administration/enforcement of the relevant statutes	No	*Personal Health Information Protection Act*
Deputy Minister of Veteran's Affairs or person with express direction	To review the information about the care received by a member of the Canadian Armed Forces	No	*Public Hospitals Act*

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Individual assessing patient capacity, who is not providing care to the patient	To assess capacity under the *Substitute Decisions Act*, *Health Care Consent Act*, or *Personal Health Information Protection Act*	No	*Substitute Decisions Act*; *Health Care Consent Act*; *Personal Health Information Protection Act*
Minister Inspector	Administration/enforcement of the *Public Hospitals Act*	No	*Public Hospitals Act*
Minister Inspector	Enforcement of the *Drug and Pharmacies Regulation Act*	No	*Drug and Pharmacies Regulation Act*
Public Guardian and Trustee	To investigate an allegation that a patient is unable to manage their property	No	*Public Hospitals Act*; *Personal Health Information Protection Act*
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	No	*Personal Health Information Protection Act*

Disclosure to Lawyers, Insurance Companies, Adjusters, Investigators

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Lawyers, Insurance Companies, Adjusters on behalf of a patient	To assist a patient with a claim or proceeding	Yes	Express consent

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Lawyers, Insurance Companies, Adjusters, Investigators on behalf of a third party, if the third party is an agent or former agent of the hospital/physician	To assist the third party with a proceeding	No	*Personal Health Information Protection Act*

Disclosure to Legal Authorities and Law Enforcement

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Head of penal or custodial institution or an officer in charge of a psychiatric facility where the patient is being lawfully detained	To assist with health care or placement decisions	No	*Personal Health Information Protection Act*
Investigator or Inspector	To conduct an investigation or inspection authorized by a warrant or law	No	*Personal Health Information Protection Act*
Police without a warrant	Legal authorities and law enforcement	Yes	Express consent
Police without a warrant	Where there are reasonable grounds to believe that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm	No	*Personal Health Information Protection Act*
Probation and Parole Services	Legal authorities and law enforcement	Yes	Express consent

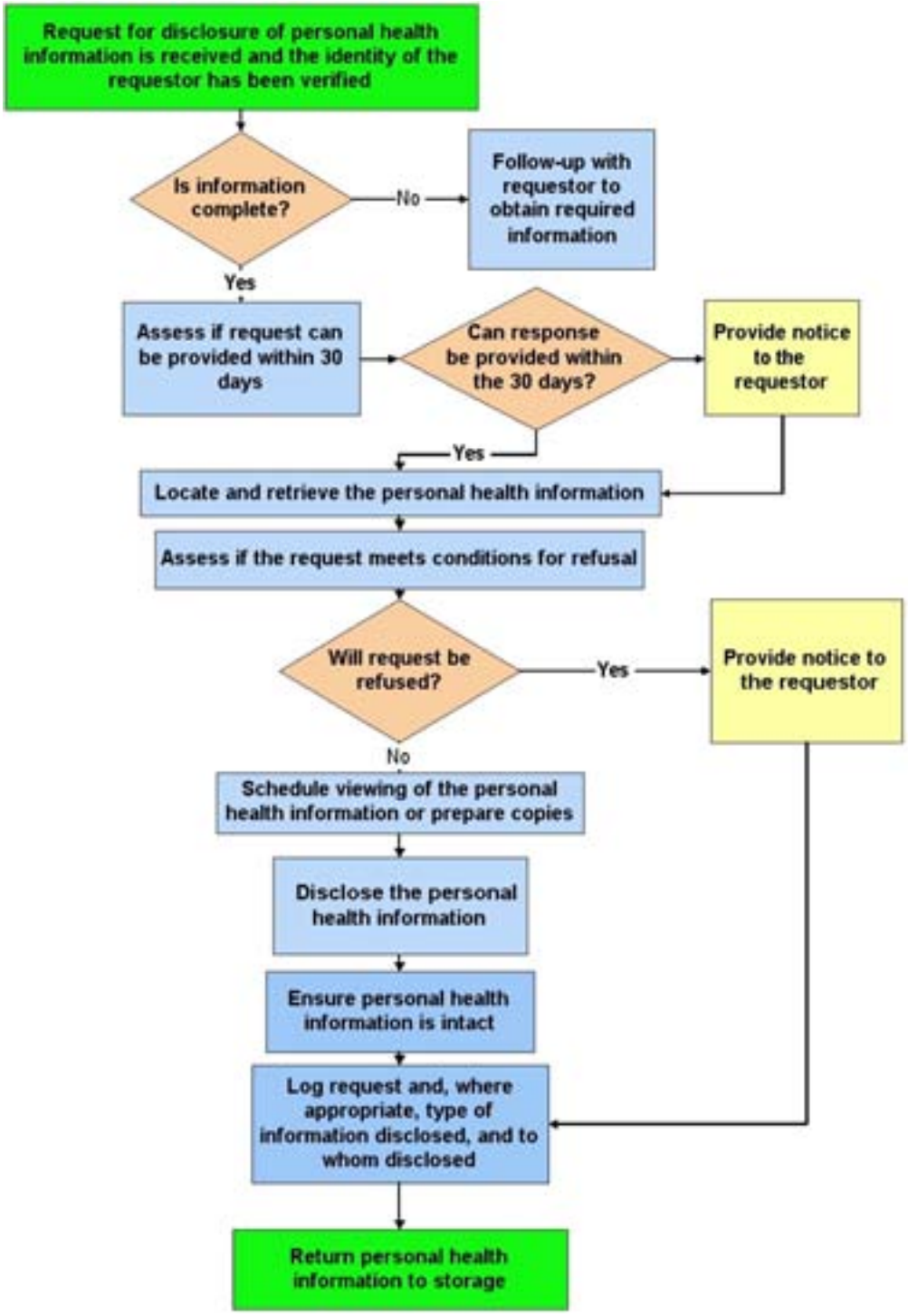
Related Sections of the Act

37, 38, 39, 40, 41, 42, 43, 43.1, 44, 45, 46, 47, 48

Checklists, Templates and Tools

- Process Map for Disclosing Personal Health Information
- Sample Non-Disclosure Agreement
- Sample Consent to Disclose Personal Health Information Form

PROCESS MAP FOR DISCLOSING PERSONAL HEALTH INFORMATION



SAMPLE CONFIDENTIALITY AGREEMENT

NOTE TO USER: Modify this sample agreement to suit your institution and your needs. Review with your lawyers before releasing.

I acknowledge that I have read and understood the **[●]** policies and procedures on privacy, confidentiality and security.

I understand that:

- all confidential and/or personal health information that I have access to or learn through my employment or affiliation with **[●]** is confidential,
- as a condition of my employment or affiliation with **[●]**, I must comply with these policies and procedures, and
- my failure to comply may result in the termination of my employment or affiliation with **[●]** and may also result in legal action being taken against me by **[●]** and others.

I agree that I will not access, use or disclose any confidential and/or personal health information that I learn of or possess because of my affiliation with **[●]**, unless it is necessary for me to do so in order to perform my job responsibilities. I also understand that under no circumstances may confidential and/or personal health information be communicated either within or outside of **[●]**, except to other persons who are authorized by **[●]** to receive such information.

I agree that I will not alter, destroy, copy or interfere with this information, except with authorization and in accordance with the policies and procedures.

I agree to keep any computer access codes (for example, passwords) confidential and secure. I will protect physical access devices (for example, keys and badges) and the confidentiality of any information being accessed.

I will not lend my access codes or devices to anyone, nor will I attempt to use those of others. I understand that access codes come with legal responsibilities and that I am accountable for all work done under these codes. If I have reason to believe that my access codes or devices have been compromised or stolen, I will immediately contact the **[●]**.

Name (Please Print)	Signature	Date

SAMPLE CONSENT TO DISCLOSE PERSONAL HEALTH INFORMATION FORM

I _____ hereby authorize _____
(Name of hospital/physician's office)

to disclose the following personal health information:

_____

_____
(Description of personal health information to be disclosed and dates of contact/hospitalization)

to _____

_____
(Name and address of person/agency requesting information)

from the records of _____
(Name of Patient) **(Birth date)**

Mailing Address of Patient: _____

_____

I understand that this personal health information is to be used **only** by the recipient for the purposes of:

_____

_____

Date: _____

I hereby waive any and all claims against **[insert name of hospital/physician's office]** in connection with the disclosure of this personal health information.

Witness: _____ Signed by: _____
(Patient or Substitute Decision-Maker)

Date: _____ _____
(Relationship to the Patient)

Accessing Health Records

Table of Contents

Accessing Health Records

Key Points

- The term “access” refers to access by patients or their substitute decision-makers.
- Subject to a few exceptions, you must provide patients (or their substitute decision-makers) with access to their personal health records in a timely manner.
- You must develop procedures to handle access requests.
- You must make available a written statement telling patients and substitute decision-makers who to contact and what to do if they want to see their personal health record.
- The Act does not prevent you from informally communicating with your patients or their substitute decision-makers.
- The access rules in the *Mental Health Act* are repealed as of November 1, 2004, and the transitional rules found in the Act apply. This means that as of November 1, 2004, you must comply with the access rules found in the Act (as opposed to those found in the *Mental Health Act*); however, if you received an access request before November 1, 2004, the access rules found in the *Mental Health Act* apply to that request.

Accessing Health Records

The Rule

Except under special circumstances, patients have the right to access their personal health records.

Patients may request access to their personal health records orally or in writing. Oral requests are routine when the patient is still receiving care, and the Act does not prohibit you from responding to oral requests. The request must be in writing, however, to invoke the rights and procedural requirements set out in the Act.

A substitute decision-maker can request access on a patient's behalf because the right of access exists whether or not a patient has capacity. Substitute decision-makers will follow the same process to obtain access to the personal health record as the patient. See the Consent section for more information on substitute decision-makers.

The Act does not prevent you from informally communicating with your patients or their substitute decision-makers. The access rules in the *Mental Health Act* are repealed as of November 1, 2004, and the transitional rules found in the Act apply. This means that as of November 1, 2004, you must comply with the access rules found in the Act (as opposed to those found in the *Mental Health Act*); however, if you received an access request before November 1, 2004, the access rules found in the *Mental Health Act* apply to that request.

Note: The term "access" refers to access by patients or their substitute decision-makers. The term "disclosure" refers to access by individuals other than patients or their substitute decision-makers. See the Collection, Use and Disclosure section for more information on disclosure to others. For the sake of brevity, the term "requestor" is used to describe patients and substitute decision-makers in this section of the Toolkit.

What You Need To Do

If you are asked for access to a personal health record:

- Verify the patient's identity or substitute decision-maker's authority.
- Determine if the request contains enough detail to let you reasonably find the record. If you need more information to find the record, work with your patient to obtain the information you require. If you cannot find the record after a reasonable search, tell the requestor so in writing.

- Determine if one of the legal exceptions applies to providing access. See the table on pages 80 to 81 for a description of where you may refuse access.
- If a legal exception applies:
  - tell the requestor in writing that you are refusing access, in whole or in part, and why you are doing so,
  - where possible, sever the record and provide access to the part of the record where no legal exception applies,
  - tell the requestor about your complaints procedure, and that if the requestor is not satisfied with your resolution of the complaint, the requestor can complain to the Commissioner, and
  - in some circumstances, you cannot even tell the requestor that a personal health record exists.

  Guidelines for refusing access are found at page 79.
- If no legal exception applies and you can find the record, arrange to provide access. You can provide access by showing the requestor the original record. If you choose to show the requestor the original record, you should arrange for the requestor to be monitored while viewing the record to ensure that it is not altered in any way. You can also provide access by giving the requestor a copy of the record. You must provide a copy if the requestor asks for a copy.
- If reasonably practical, answer any questions about any medical terms or abbreviations used in the record.
- Put policies and procedures in place to handle access requests.
- Make available a written statement telling patients and substitute decision-makers who to contact and what to do if they want to see their personal health record. See the General Privacy Compliance and Contact Person sections for more information on the written statement and the contact person.

What You Should Do

- Train all staff to direct a requestor to your contact person if they want access to a personal health record.
- Forward all access requests to your contact person. The contact person can also help to complete a request form for access to the personal health record.

- Document the date of the request for access in the patient's personal health record.

The Sample Checklist – Process for Accessing a Personal Health Record provides a sample procedure for processing access requests.

Fees for Providing Access

You may charge a fee to provide access to a personal health record if you first give the requestor an estimate of the fee.

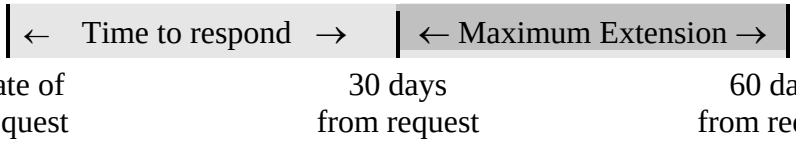
The fee you charge cannot exceed either a prescribed amount or, if no amount is prescribed, a reasonable cost recovery charge.

You may waive payment of all or any part of the fee if it is fair to do so.

Note: The Regulations do not currently prescribe a fee.

Timeframe to Respond to a Request for Access

Respond to requests for access as soon as possible. If you need more than 30 days to respond to a request for access, provide the requestor with written notice of an extension.



An extension is only permitted if:

- replying to the request within 30 days would reasonably interfere with your activities because locating the personal health record requires a complex search, or
- the time required to undertake the necessary consultations would make it reasonably impractical to reply within 30 days.

The written notice of an extension should explain:

- when you will respond, and
- why an extension is needed.

An extension cannot exceed an additional 30 days.

If you do not provide access within the stated time period, the requestor can assume that you have refused the request.

Urgent Requests for Access

If a requestor can satisfy you that the request is urgent, you must provide access within the requested time period, if it is reasonable to do so.

Refusing a Request for Access

The table below lists circumstances where you may refuse access to personal health records.

Even when a restriction to access exists, a requestor has a right to access personal health information not related to the restriction. You must sever the restricted information from the rest of the record, and give the requestor access to the remaining information.

You should tell requestors that their request has been refused and, where appropriate, give reasons for the refusal. There may be situations where access is refused and you do not confirm or deny the existence of a record. This is context specific and you may need to confer with a psychologist, legal counsel or the Commissioner about how reasons for your refusal should be communicated.

You should tell requestors that they can complain about your refusal to the Commissioner. You should also provide information on how to contact the Commissioner.

Guidelines for Refusal of Access

In each of the following situations, you should provide access to the part of the record that is not impacted by the reason for refusal and that can reasonably be severed from the record.

Reason for Refusal of Access	Follow-Up Notification to Requestor	
	State you are refusing the request (in whole or in part) and reason for the refusal	**State you are refusing to confirm or deny the existence of any record**
The record contains quality of care information	×	
The record contains information collected/created to comply with the requirements of a quality assurance program under the *Health Professions Procedural Code* that is Schedule 2 to the *Regulated Health Professions Act*	×	
The record contains raw data from standardized psychological tests or assessments	×	
The record (or information in the record) is subject to a legal privilege that restricts disclosure to the requestor	×	
Other legislation or court order prohibits disclosure to the requestor	×	
The information in the record was collected/created in anticipation of or use in a proceeding that has not concluded		×
The information in the record was collected/created for an inspection/investigation/similar procedure authorized by law that has not concluded		×
Granting access could reasonably be expected to result in a risk of serious harm to the patient or to others (Where this is suspected you may consult a physician or psychologist before deciding to refuse access)		×

Reason for Refusal of Access	Follow-Up Notification to Requestor	
	State you are refusing the request (in whole or in part) and reason for the refusal	**State you are refusing to confirm or deny the existence of any record**
Granting access could lead to the identification of a person who was required by law to provide the information in the record		×
Granting access could lead to the identification of a person who provided the information in the record in confidence (either explicitly or implicitly) and it is considered appropriate to keep the name of this person confidential		×
The request for access is frivolous, vexatious or made in bad faith	×	
The identity or authority of the requestor cannot be proven by the requestor	×	

Failing to Respond to a Request for Access

If you fail to respond to a request for access within the time required by the Act, you will be deemed to have refused the request.

Requestors can complain to the Commissioner about your refusal of a request for access. You will have to justify your decision to refuse access.

It is an offence under the Act to dispose of records so that you do not have to respond to a request for access. You may face penalties if you commit this offence.

Related Sections of the Act

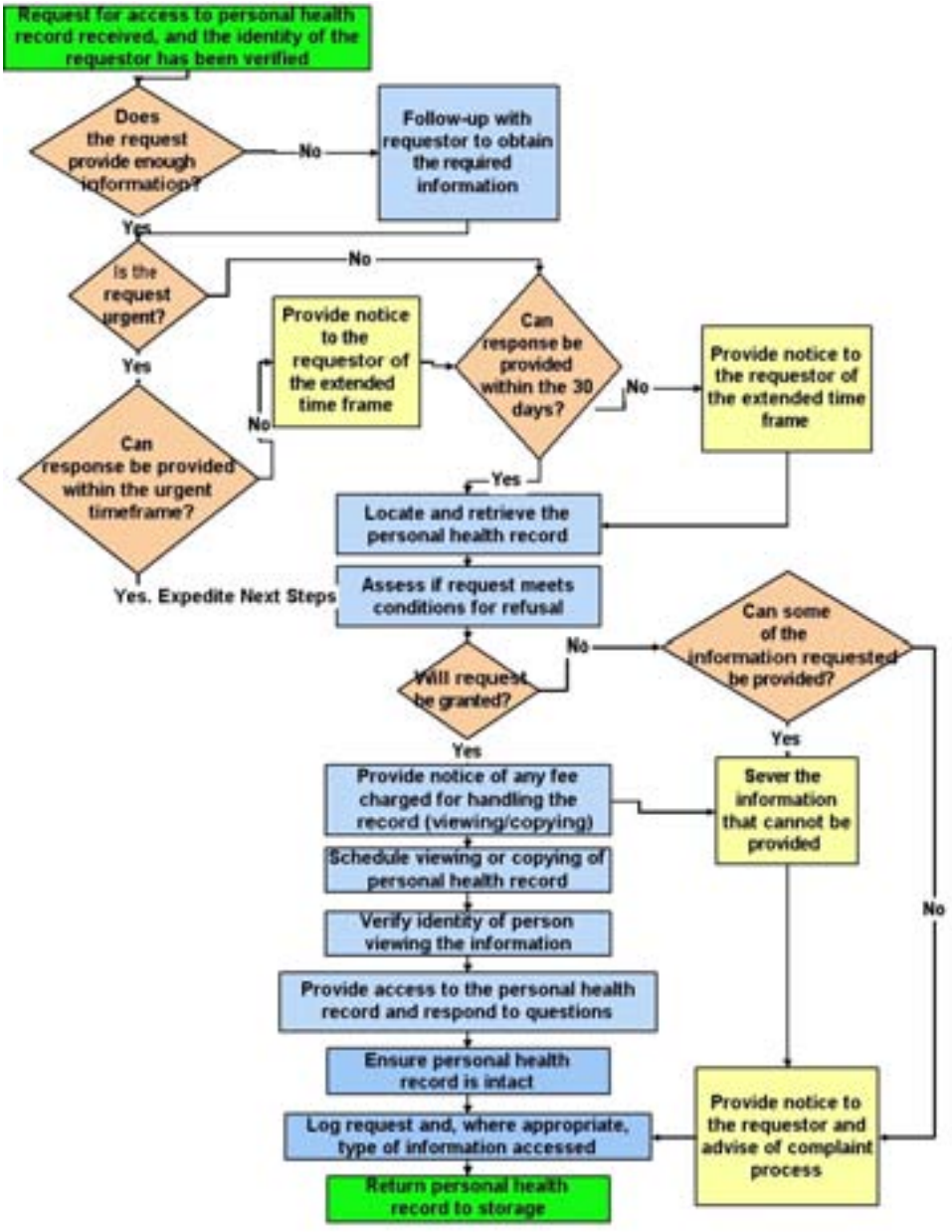
51, 52, 53, 54, 72 (1)(d)

Accessing Health Records

Checklists, Templates and Tools

- Sample Process Map – Access to Personal Health Record
- Sample Form to Request Access to Personal Health Record
- Sample Checklist – Process for Accessing a Personal Health Record
- Sample Letter for Extension to Comply with Request
- Sample Refusal of Access Letter

SAMPLE PROCESS MAP
– ACCESS TO PERSONAL HEALTH RECORD



SAMPLE FORM TO REQUEST ACCESS TO PERSONAL HEALTH RECORD

Information and Instructions

We will provide you with access to your personal health record, unless a legal exception applies. We will review all health record access requests, and will make every effort to respond to your request in a timely fashion. Please complete Parts A and B of this Form. Part C is for our internal use. For information about our privacy protection practices, contact ● at: **[Address, fax, email and telephone number.]**

PART A: REQUESTOR INFORMATION

Patient Contact Information:

Last Name _____ First Name _____ Initials _____

Mailing Address _____

Telephone Number _____ Date of Birth _____

Hospital ID Number _____

If you are a substitute decision-maker, your contact information:

Last Name _____ First Name _____ Initials _____

Mailing Address _____

Telephone Number _____

Note: Include copies of documents that provide your authority as a substitute decision-maker.

PART B: ACCESS REQUEST

1. Please describe what you need and include details that will help us locate the record (e.g., dates, name of healthcare provider, etc.).

_____

_____

_____

2. How would you prefer to access this information? Please check off:

- ☐ Receive hard copies of originals
- ☐ Receive electronic copies of originals (please supply storage medium)
- ☐ Examine originals in the facility

Signature	Name (print)	Date

PART C: RESPONSE TO ACCESS REQUEST (For Internal Use Only)

1. Information Regarding Receipt and Initial Review of Request

Date Request Received

2. Information Regarding Response

Date Response Issued

- ☐ Access request granted
- ☐ Access request not granted
- ☐ Access request granted in part

If complete access request was not granted, reason for refusing the request/part of the request.

3. Information Regarding Extension

If an extension to the access request response was required, please indicate:

Date of Extension	Reason for Extension	Date Patient Notified

4. Processed by:

Signature	Name (print)	Title

SAMPLE CHECKLIST – PROCESS FOR ACCESSING A PERSONAL HEALTH RECORD

☐ Give the requestor a form to **request access to the health record** (in whole or part) or inform them of what to include in a written request. An oral request may also be accepted. See Checklist for Information to Include in a Request Form.

☐ **Verify the identity** of the requestor.

Verification of an Oral Request – Patient	**Verification of a Written Request – Patient**	**Verification of a Written Request – Substitute Decision-Maker**
Request photo-ID for verification purposes if patient is not known You should only accept requests by phone if you know the patient If practical, call back to verify the patient's identity	Ensure the following patient information from the request matches information in your registration system: • name • date of birth • hospital ID number Check that a signature is included	Review information in the health record to ensure there is documentation that the requestor is a substitute decision-maker Request documentation (power of attorney) if there is no information in the health record Verify if any parent requesting access for a minor is the custodial parent and that the parent is entitled to access

☐ Once you have the request, make sure you have **enough information** and any required payment to allow you to find the health record.

If you need more information, follow up with the requestor.

Fee estimates should be provided and agreed upon in advance. If payment is required, ensure the fee is included, otherwise follow up. Do not charge fees over a prescribed amount. If there is no prescribed amount, do not charge more than what you need to recover costs. You may waive any fees.

☐ Decide if there are any reasons to **refuse access to the health record** (in whole or part). See Guidelines for Refusal of Access.

☐ If the health **record cannot be located**, provide a written notice/form to the requestor advising them that the health record either does not exist or cannot be found.

☐ Assess if the request is **urgent** (required in fewer than 30 days of initial request).

Expedite request if the requestor can show that the need is urgent and you have enough time to respond.

If you cannot meet the timeframe requested, advise the requestor.

☐ Assess if the **request for access can be provided within 30 days** of receipt of the request.

If an extension is needed, provide a written notice/form to the requestor advising of the reason for the delay and length of the extension. The length of the extension must not exceed 30 days, and is only permitted in certain circumstances.

☐ If **access is denied**, provide a written notice to the requestor. Make sure the notice reflects the appropriate response (see Table included in the Guidelines for Refusal of Access).

☐ **Retrieve the health record**.

☐ **Provide a copy of the record** or **schedule a convenient time** for the requestor to look at the requested health record (or copy) in a private and secure location.

☐ Ensure you **verify the identity** of the requestor who comes in to examine the health record. See Table above for guidelines.

☐ **Ensure the health record remains secure**. Information in the health record should not be removed, changed or otherwise tampered with. Supervise the requestor viewing the health record to ensure the health record remains intact.

☐ Where it is reasonable, respond to any questions about **medical terms or abbreviations**.

☐ **Verify the health record is intact** and **return the health record to its filing location**, as needed.

☐ **Document** all requests, extensions, accesses and refusals to access the health record. Ensure an event record is created when a requestor views an electronic health record.

SAMPLE LETTER FOR EXTENSION TO COMPLY WITH REQUEST

[Name and Address of Health Care Facility]
XXX Street
City/Town, Ontario
ABC 123

Date

Dear Sir/Madam,

RE: Request for Access to Personal Health Record of [Patient's Name]

Health Record #:

An extension of _____ days is required to address your request to access the personal health record of the individual named above. While every effort is made to retrieve the information requested, this extension is required for the following reason:

[Reason for extension]

If you have any concerns or questions please contact _____ (Contact Person). If they are unable to resolve your concerns, you may file a complaint with the Information and Privacy Commissioner/Ontario, who may be contacted at:

[Contact information for the Information and Privacy Commissioner/Ontario]

Sincerely,

_____
[Name, Title]

SAMPLE REFUSAL OF ACCESS LETTER

[Name and Address of Health Care Facility]
XXX Street
City/Town, Ontario
ABC 123

Date

Dear Sir/Madam,

RE: Request for Access to Personal Health Record of [Patient's Name]

Your request for access to the personal health record has been declined for the following reason:

[Reason for declining request]

If you have any questions or concerns please contact _____ (Contact Person). If we are unable to resolve your concerns, you may contact the Information and Privacy Commissioner/Ontario, who may be contacted at:

[Contact information for the Information and Privacy Commissioner/Ontario]

Sincerely,

_____

[Name, Title]

Correcting Health Records

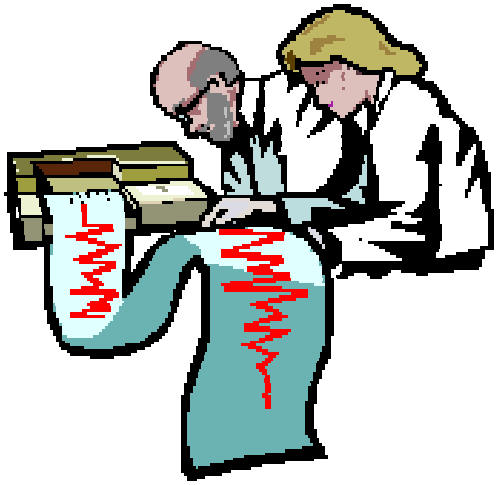


Table of Contents

Correcting Health Records

Key Points

- Subject to a few exceptions, you must correct a patient's health record at the patient's request in a timely manner, if the requirements set out in the Act are met.
- You must develop procedures to handle correction requests.
- You must make available a written statement telling patients and substitute decision-makers who to contact and what to do if they want to correct their personal health record.
- The correction rules in the *Mental Health Act* are repealed as of November 1, 2004. This means that as of November 1, 2004, you must comply with the corrections rules found in the Act (as opposed to those found in the *Mental Health Act*).

Correcting Health Records

The Rule

If you have granted a patient access to his or her personal health record and the patient thinks that the record is not correct or complete for your purposes, the patient may ask you (in writing) to correct the record.

If the patient makes an oral request for a correction, you may respond to it; however, only written requests invoke the rights and procedural requirements set out in the Act.

With a few significant exceptions, you must make the requested correction if the patient can show to your satisfaction that the record is not correct or complete for your purposes and also gives you the information you need to make the correction.

A substitute decision-maker can request a correction on a patient's behalf because this right exists whether or not a patient has capacity. Substitute decision-makers will follow the same process to request a correction to the personal health record as the patient. See the Consent section for more information on substitute decision-makers. The correction rules in the *Mental Health Act* are repealed as of November 1, 2004. This means that as of November 1, 2004, you must comply with the corrections rules found in the Act (as opposed to those found in the *Mental Health Act*).

What You Need To Do

- Put policies and procedures in place to handle correction requests.
- Make available a written statement telling patients and substitute decision-makers who to contact and what to do if they want to correct their personal health record. See the General Privacy Compliance and Contact Person sections for more information on the written statement and the contact person.

Responding to Requests for Correction

If you receive a written request for a correction, you should:

- Verify the patient's identity or substitute decision-maker's authority.
- Verify that the patient or substitute decision-maker has a right of access to the personal health record.

- Ensure the request for correction relates to a personal health record created by you or your staff.
- Determine who will validate the request and correct the personal health record. Confirm that this person has the knowledge, expertise and authority to validate and make the correction.

When making a correction you must:

- record the correct information in the record, and
- cross out the incorrect information (without obliterating it) or, if that is not possible, label the information as incorrect, remove it and store it separately from the record, and keep a link in the record that lets you trace the incorrect information.

If it is not possible to record the correct information in the record, you must put a practical system in place to:

- inform anyone who uses the record that the information in the record is incorrect, and
- direct that person to the correct information.

Once you correct the personal health record:

- tell the patient in writing how the correction was made, and
- if the patient asks you to do so and to the extent reasonably possible, tell others in writing to whom you have disclosed the incorrect information of the correction, unless the correction cannot reasonably be expected to affect the ongoing provision of health care or otherwise benefit the patient.

What You Should Do

- Develop procedures to determine who should assess requests for correction and make corrections.
- Where practical, refer the request for correction to the author of the personal health record unless the author is not available, there is a question of competence or negligence in the creation of the record or if the patient has specifically requested that another practitioner assess the record.
- If appropriate, refer the request to the most responsible physician.
- Date and sign corrections.
- Advise any members of the patient's circle of care of the correction if it affects the patient's current plan of care.

- Notify anyone who is currently using the personal health record of the correction.

Where You Do Not Have To Make Corrections

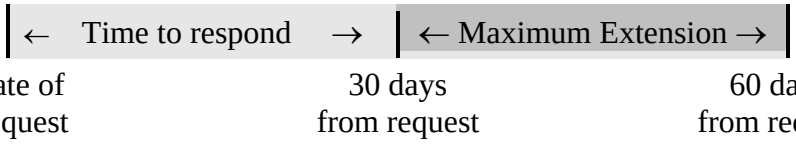
You do not have to correct a record:

- that was not made by you/your facility and where you do not have sufficient knowledge, expertise and authority to correct the record (this would include your ability to validate the new information being provided),
- if you reasonably believe that the request for correction is frivolous, vexatious or made in bad faith (requests should only be refused for these reasons in the rarest of cases),
- if the patient has failed to demonstrate that the record is not correct or complete, or
- if the patient has not given you the information you need to make the correction.

You do not have to correct a professional opinion or observation made in good faith about a patient.

Timeframe for Responding to a Request for Correction

Respond to requests for correction as soon as possible and within 30 days of your receipt of the request. If you need more than 30 days to respond to a correction request, give the patient a written notice of an extension.



An extension is only permitted if:

- replying to the request within 30 days would unreasonably interfere with your activities, or
- the time required to undertake the necessary consultations would make it reasonably impractical to reply within 30 days.

The written notice of an extension must describe:

- when you will respond, and
- why an extension is needed.

An extension cannot exceed an additional 30 days.

If you do not make a correction within the stated time period, the patient can assume that you have refused the request.

Conflict Resolution: Refusing a Request for Correction

If you refuse a request, tell the patient in writing:

- the reason for your refusal, and
- that the patient can:
  - prepare a brief written description of the correction that you refuse to make,
  - require you to attach this document to the patient's personal health record, and make you disclose the document whenever you disclose the information to which it relates,
  - require you to make all reasonable efforts to disclose this document to anyone to whom the patient's personal health record had been disclosed, unless the correction cannot reasonably be expected to affect the ongoing provision of health care or otherwise benefit the patient, and
  - complain about your refusal to the Commissioner.

Note: The patient also has these rights when you are deemed to refuse a request.

If you refuse a request because you think it is frivolous, vexatious or made in bad faith, tell the patient in writing:

- the reason for your refusal, and
- that the patient can complain about your refusal to the Commissioner.

Related Sections of the Act

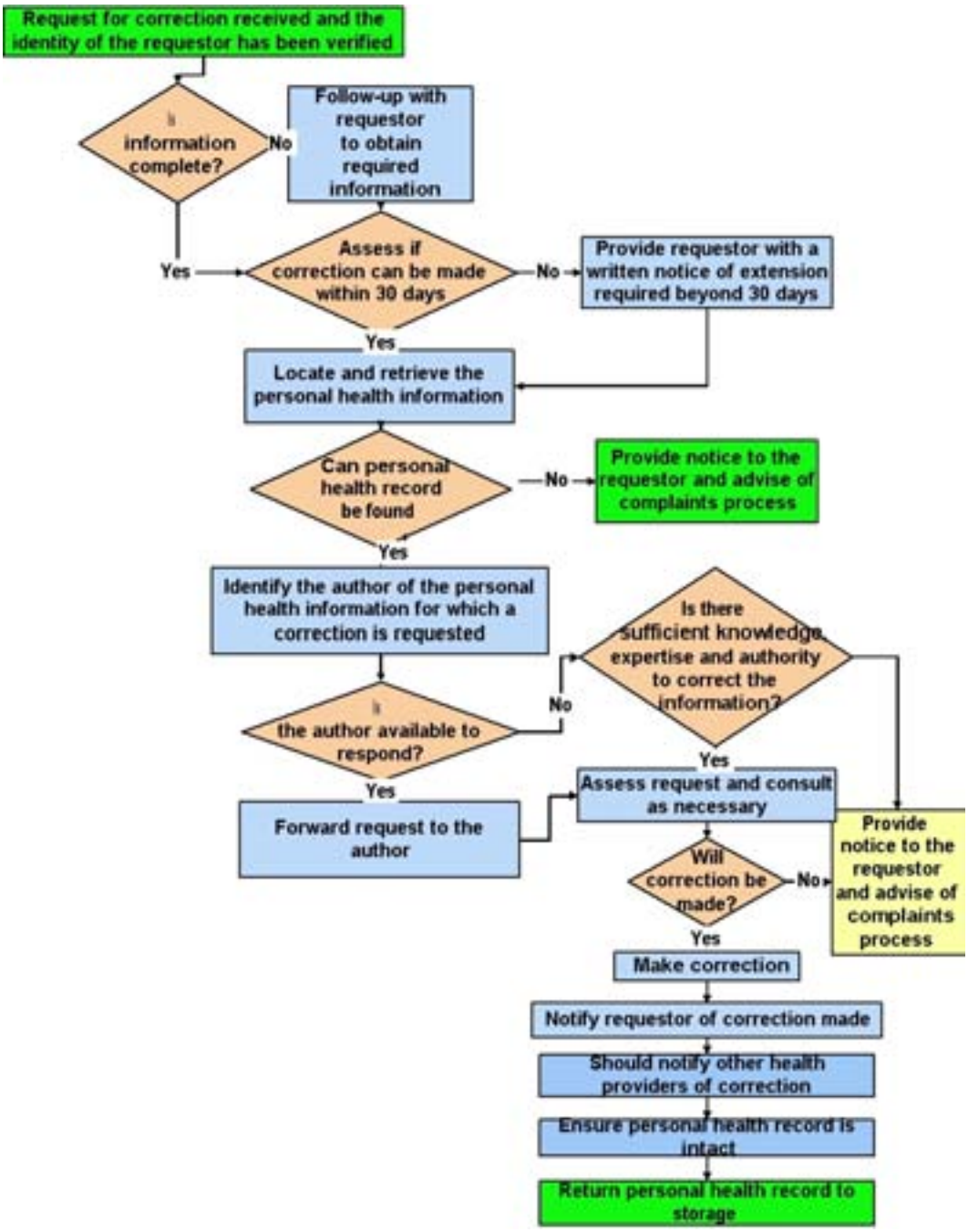
55

Checklists, Templates and Tools

- Process Map for Responding to Requests for Correction
- Sample Request Form for Correction to Personal Health Record

Correcting Health Records

PROCESS MAP FOR RESPONDING TO REQUESTS FOR CORRECTION



SAMPLE REQUEST FORM FOR CORRECTION TO PERSONAL HEALTH RECORD

Information and Instructions

We will correct health record information if it is demonstrated, to our satisfaction, that the record is not correct or complete for the purpose for which we collect, use or disclose the information. We will make every effort to respond to your request in a timely fashion. Please complete Parts A and B of this Form. Part C is for our internal use. For information about our privacy protection practices, contact **[●]** at: **[Address, fax, email and telephone no.]**

PART A: REQUESTOR INFORMATION

Patient Contact Information:

Last Name _____ First Name _____ Initials _____

Mailing Address _____

Telephone Number _____ Date of Birth _____ Hospital ID Number _____

If you are a substitute decision-maker, your contact information:

Last Name _____ First Name _____ Initials _____

Mailing Address _____

Telephone Number _____

Note: Include copies of documents that provide your authority as a substitute decision-maker.

PART B: CORRECTION REQUEST

1. List or attach the correction requested, with reasons for the correction.

Requested Correction	**Reasons for Correction**

2. How do you wish to receive notice of the correction (in writing, by telephone)? _____

3. Would you like us to give notice of the correction, to the extent reasonably possible, to others to whom we have disclosed the incorrect information? (We will only do so if this notice will affect your health care or otherwise benefit you.)

☐ Yes
☐ No

Signature _____ Name (print) _____ Title _____

Date _____

PART C: CORRECTION REQUEST RESPONSE (For Internal Use Only)

☐ Correction made
☐ Correction not made
☐ Refusal letter (with reasons) sent
☐ Statement of Disagreement attached to record
☐ Date of Response _____

1. List names, contact information and comments of any individuals consulted

_____

2. If correction was not made, provide reasons:

_____

3. If an extension to the correction request response was required, please indicate:

Date of Extension	Reason for Extension	Date Patient Notified of Extension

4. Notice of correction provided to others to whom incorrect information was disclosed. List names:

5. Processed by:

Signature _____ Name (print) _____ Title _____

Dealing with Health Information

Table of Contents

Dealing with Health Information

Key Points

- You must store your patients' personal health information in a reasonably secure manner and in accordance with the prescribed requirements, if any.
- If your patients' personal health information is stolen, lost or accessed by unauthorized persons, you must notify your patients as soon as possible.
- You must retain personal health records for their minimum retention periods, and as long as needed to allow patients to exhaust any legal recourse available to them involving an access request.
- You must dispose of your patients' personal health records in a secure manner.
- You may transfer your patients' personal health records as described in the Act so long as you do so securely.

Storage and Retention

The Rule

Storage

You must store your patients' personal health information in a reasonably secure manner and in accordance with the prescribed requirements, if any.

If your patients' personal health information is stolen, lost or accessed by unauthorized persons, you must notify your patients as soon as possible. (There is an exception under the law for researchers. See the Research section for details.)

Retention

The Act does not establish specific retention periods, but does require records containing personal health information to be kept:

- no longer than prescribed by law, and
- for as long as needed to allow a patient to exhaust any legal recourse a patient has regarding a request for access.

Note: The Regulations made under the Act do not currently contain any specific storage or retention rules; however, the Regulations made under the *Public Hospitals Act* that deal with record retention do continue to apply.

What You Need To Do

- Retain your patients' personal health information in a reasonably secure manner. See the Security section for guidelines on keeping information secure.

- The steps you take must address your:
  - physical security (for example, locked filing cabinets, restricted office access and alarm systems),
  - technological security (for example, passwords, encryption and firewalls), and
  - administrative controls (for example, security clearances, access restrictions, staff training and confidentiality agreements).

Note: If you are a physician and you keep electronic health information, make sure you:

- can display and print your records for each patient in chronological order,
- can retrieve your records by the patient's name and health card number (where applicable),
- keep an audit trail that:
  - records the date and time of each entry for each patient,
  - shows any changes in the record,
  - preserves the original record's content when changed or updated, and can be printed separately from other patients' records,
- use password protection or other features to secure the records from unauthorized access, and
- install automatic back-up for file recovery to protect your records from loss and damage.

- Retain personal health records for their minimum retention periods. This means in every instance you need to know the retention periods various laws prescribe and why the information you are dealing with was collected.
- When patients have requested access to their own personal health records, retain those records as long as needed to allow the patients to exhaust any legal recourse involving the request.

What You Should Do

- Establish procedures for record storage. These procedures should be based on the guidelines provided in the Security section.
- Establish procedures for record retention. These procedures should be based on the information in the Summary of Retention Periods.
- Retain clinical records for the periods described in the Summary of Retention Periods. Retain educational, administrative, funding and research records for as long as you need them to serve their purpose, and then securely dispose of them.
- In deciding how long you need to keep your patients' personal health information, follow three steps:
  - First, consider why you collected the information (for example, for research, funding or clinical purposes).
  - Second, consider how long the law requires you to keep the records.
  - Third, decide whether under the circumstances you should hold onto the records longer than required to manage legal risks (for example, where patients have sued in the past).
- A general practice is to retain information for 10 years from the time the record was last updated or from when a minor attained the age of majority.
- Consider your own risk management. What if a patient sues you after the minimum retention period has ended and you have destroyed records that could help defend you? Before disposing of files, ask yourself whether the patient's case was one that might lead to a lawsuit. For example, certain kinds of treatment have a higher incidence of negligence claims (such as gynaecology and obstetrics). You may want to retain these records for longer periods than legally required.
- See the Summary of Retention Periods for retention periods for:
  - Health Records
  - OHIP Records
  - Research Records
  - Education Records

Disposal

The Rule

You must dispose of your patients' personal health records in a secure manner. The Act does not specify disposal methods.

What You Need To Do

- Dispose of your patients' personal health records in a secure manner.

What You Should Do

- Outline very clear procedures for securely disposing of personal health records and make sure your procedures are always followed.
- For hard copy records, secure disposal means shredding or burning them.
- For electronic records, secure disposal means either physically destroying the media they are stored on (such as a CD) or magnetically erasing or over-writing the information (in such a way that it cannot be recovered). Encrypting information is not a method of disposal even if the encryption keys are destroyed because it is possible that encrypted information may be recovered at some time in the future, even though keys have been destroyed.
- For more information on the security aspects of record disposal, see Security – People – Personal Responsibilities for Security.
- When you dispose of personal health records, record:
  - the names of the patients whose records were disposed of,
  - the dates the records were disposed of, and
  - that you properly followed your hospital's disposal procedures.

  Keep this record of disposal for as long as your hospital by-laws require.

  Note: This is a requirement of the *Public Hospitals Act*.

Transfer

The Rule

You may transfer your patients' personal health records as described in the Act so long as you do so securely.

What You Need To Do

Transfer to Another Facility

- When you transfer your patient's personal health records to another facility or physician, you must keep the original record and only transfer a copy.

  Note: This is a requirement of the *Public Hospitals Act* and the *Medicine Act*.

Transfer to a Successor

- When you transfer your patients' personal health records to your successor, make reasonable efforts to notify your patients before transferring their records or, if that is not reasonably possible, as soon as possible afterwards.

Transfer to Archives

- When you transfer your patients' personal health records to:

  – the Archives of Ontario, or

  – in certain prescribed circumstances, a prescribed person whose duties include collecting and preserving records of historical or archival importance, if the transfer is made for that purpose,

  make sure you have the archivist's agreement to the transfer.

  Note: In this context, the transfer is made for storage purposes.

What You Should Do

- Follow the guidance provided in the Security section to make sure you are transferring information securely.

Related Sections of the Act

Sections 2, 3, 4, 10, 12, 16, 17, 42, 52, 72 of the Act

Sections 1(10), 14 of the General Regulation

Checklists, Templates and Tools

Summary of Retention Periods

See the Security section for additional checklists, templates and tools.

SUMMARY OF RETENTION PERIODS

Retention Periods for Health Records for Hospitals

Patient Care Records:

Adults	10 years after the patient's discharge or death (inpatient), or 10 years after the patient's last visit or death (outpatient)
Minors	10 years after the day the patient turns or would have turned 18

Diagnostic Imaging Records:

Adults	5 years after the day the record was created, except for diagnostic imaging records of a breast examination, which must be retained for 10 years
Minors	5 years after the day the patient turned 18, except for diagnostic imaging records of a breast examination, which must be retained for 10 years after the patient turns 18

Adults and Minors:

Videotapes of diagnostic imaging examinations need not be kept unless the videotape constitutes the only record of the examination

Investigations

If a notice for an investigation or inspection under the *Regulated Health Professions Act*, *Health Insurance Act* or *Coroners Act* is received, the records must be retained until the investigation or inspection and any subsequent hearing is completed

Patient Access Requests

A personal health record cannot be disposed of if the patient the record relates to seeks access to those records and has not yet exhausted all avenues allowing for access

Lawsuits

Where a claim of negligence may arise:

Adults:	A minimum of 15 years from the date on which the act or omission upon which the claim of negligence could be based occurred
Minors:	A minimum period of 15 years from the date the patient turned 18

In both cases, if the patient cannot commence a claim because of a mental, physical or psychological condition and the individual has no litigation guardian, the records should be kept longer

The rules around discoverability of a negligence claim are complex and are dependent on the specific facts of each case

For specific retention periods regarding individual cases, consult your lawyer

Retention Periods for OHIP Records for Hospitals

The *Health Insurance Act* requires that records be maintained to demonstrate that:

- an insured service was provided
- the hospital provided these services
- the service was medically and therapeutically necessary

A minimum of 10 years, in line with statutory retention periods for clinical records, to assist in proving billing was necessary

Retention Periods for Research Records for Hospitals

General Principle

Identifying data should be retained only as long as necessary to fulfill the research purpose; however,

- in a case where a claim of negligence may arise, records should be kept longer
- due to the complexity of the discoverability rules in relation to claims of negligence, for record retention periods for specific research projects, consult your lawyer

If research is conducted without patient consent, the researcher receiving the information must follow any return restrictions imposed by the originating health information custodian

Retention Periods for Health Records for Physicians (Private Office Records)

Patient Care Records:

Adults:	10 years after the last entry date, or until the physician stops practicing
Minors:	10 years after the day the patient turns or would have turned 18 or until the physician stops practicing

Special Notes:

Family medicine and primary care physicians should refer to special transfer and disposition rules if they plan to stop practicing

Dispensing physicians should refer to Supplementary Tables A and B for retention rules relating to dispensing medications

Investigations

If a notice for an investigation or inspection under the *Regulated Health Professions Act, Health Insurance Act* or *Coroners Act* is received, the records must be retained until the investigation or inspection and any subsequent hearing is completed

Patient Access Requests

A personal health record cannot be disposed of if the patient the record relates to seeks access to those records and has not yet exhausted all avenues allowing for access

Lawsuits

Where a claim of negligence may arise:

Adults:	A minimum of 15 years from the date on which the act or omission upon which the claim of negligence could be based occurred
Minors:	A minimum period of 15 years from the date the patient turned 18

In both cases, if the patient cannot commence a claim because of a mental, physical or psychological condition and the individual has no litigation guardian, the records should be kept longer

The rules around discoverability of a negligence claim are complex and are dependent on the specific facts of each case

For specific retention periods regarding individual cases, consult your lawyer

Retention Periods for OHIP Records for Physicians

The *Health Insurance Act* requires that records be maintained to demonstrate that:

- an insured service was provided
- the physician provided these services
- the service was medically and therapeutically necessary

A minimum of 10 years, in line with statutory retention periods for clinical records, to assist in proving billing was necessary

Retention Periods for Research Records for Physicians

General Principle

Identifying data should be retained only as long as necessary to fulfill the research purpose; however,

- in a case where a claim of negligence may arise, records should be kept longer

- due to the complexity of the discoverability rules in relation to claims of negligence, for record retention periods for specific research projects, consult your lawyer

If research is conducted without patient consent, the researcher receiving the information must follow any return restrictions imposed by the originating health information custodian

SUPPLEMENTARY TABLE A

RETENTION PERIODS FOR RECORDS RELATING TO DRUGS DISPENSED UNDER THE ONTARIO DRUG BENEFIT PLAN

Document	Retention Period
Statement of daily transaction totals	2 years from the statement preparation date
Summary remittance or reject statement from the Minister	2 years from the statement receipt date
Claim for payment or reversal submitted to the Ministry, with a record of the claim submission date	2 years from the claim submission date
Monthly Ontario drug benefit eligibility card or copy of the cards for each eligible person for whom a drug is dispensed	2 years from the first drug dispensing date
Prescription with a no substitution direction and accompanying copy of the Health Canada adverse drug reaction form	2 years from the receipt date
Ministry confirmation that drug is to be supplied if it meets the applicable clinical criteria set out in Part III of the Formulary	2 years from the confirmation receipt date
For each extemporaneous preparation supplied for an eligible person, the formula, including the compounding time, all of the ingredients and the quantities and cost of those ingredients	2 years from the supply date
Where the acquisition cost of a drug is claimed, a copy of the supplier's invoice and a detailed calculation in accordance with section 14 of the cost of purchasing the drug product	2 years from the receipt date

SUPPLEMENTARY TABLE B

RETENTION PERIODS REQUIRED FOR PATIENT RECORDS RELATING TO DISPENSING OF DRUGS UNDER *THE DRUGS AND PHARMACIES REGULATIONS ACT*

Document	**Retention Period**
Required dispensing records	6 years after the last entry date or until the physician stops practicing

Security – Introduction

The Rule

You must implement reasonable physical, technical and administrative measures to safeguard personal health information.

You must implement these measures to ensure the security and confidentiality of personal health information. Specifically, you must:

- prevent unauthorized use, copying or disclosure of the information,
- protect the information during collection, storage, transfer and disposal, and
- protect the integrity of the information by preventing unauthorized modification or disposal.

You must also notify your patients as soon as possible if their personal health information is stolen, lost or accessed by unauthorized persons.

The Act does not prescribe specific security standards and safeguards; instead it asks you to take reasonable steps. What is reasonable depends on the threats, risks and vulnerabilities to which the information is exposed, on the sensitivity of the information and on the extent to which it can be linked to an identifiable individual. What is reasonable can also be judged by comparing the steps you take with the best practices that other similar organizations with effective security have implemented.

It is clear that taking reasonable steps includes implementing systems and controls that safeguard how you collect, use, modify, disclose, retain, transfer and dispose of personal health information. These steps cover:

- physical security (for example, locked filing cabinets, restricted office access and alarms),
- technical security (for example, passwords, encryption and firewalls), and
- administrative controls (for example, security clearances, access restrictions, staff training and confidentiality agreements).

The four security sections that follow are designed to help you identify and implement best practices for safeguarding personal health information. When you read them, you will see statements such as “What you need to do…” You should interpret this as “What you need to do to implement best practices for

safeguarding personal health information" as opposed to "What you must do to comply with the law". Ultimately, it is up to you to decide what taking reasonable safeguard steps means for your organization, but we strongly suggest that adopting best practices is the approach to take. Clearly, if you take no steps, you are in violation of the Act.

As you read the four security sections, you should keep in mind some simple principles of security that will help you make decisions and determine priorities:

- Take a "**defence in-depth**" approach that assumes no single measure is perfect. So if it fails, you have other lines of defence to maintain protection. Consider mixing your measures between technical/physical measures and administrative measures (people and processes). Just having all technical measures could leave you exposed in situations such as power failures.

- Make sure your security program is **balanced and comprehensive**. Security is only as strong as the weakest link. Paying too much attention to one vulnerability at the expense of others will leave you exposed and will not provide you with the best value for your security dollar. It is better to have a $50 lock on both front and back doors than a $1,000 lock on the front door and none on the back.

- Don't rely **only** on technology. Using technology will be important to help you protect personal health information but people and processes are often more important. Technology is useless if people don't use it properly. And unfortunately, your people will often likely be the cause of security problems. So having informed, motivated staff using well designed processes is critical.

- Security is not just the job of the security professionals – **security is everyone's job**. Once someone has "security" in their job title you may think you can relax and assume that they are taking care of everything. Staff must be made aware that they are all key to good security.

- Keep personal health information in **places you can best protect it**. This sounds obvious but there are choices you can make to centralize the storage of both hardcopy and electronic information in areas that have good security controls such as supervised filing areas or servers managed by an IT department. Wherever possible, avoid letting the information be stored where you have less control, such as individual offices or personal computers.

You should also apply your thinking to everyone who has access to personal health information within the institution, including employees, agents, contractors and volunteers. Throughout these sections we will collectively refer to these people either as "staff", or "user" if we are talking about electronic access to information. You must also think beyond your boundaries to how the security

protections will apply to third parties who handle personal health information on your behalf.

In the next four sections, we'll deal with the critical aspects of an effective security program:

- Section 1: Security – First Steps
    - Security Program and Policy
    - Roles and Responsibilities
    - Information Inventory and Classification
- Section 2: Security – People
    - Personal Responsibilities for Security
    - Authentication and Authorization
- Section 3: Security – Institutional Safeguards
    - Perimeter Security
    - Malicious Software
    - Wireless and Portable Devices
- Section 4: Sustaining Security
    - Business Continuity
    - Development and Maintenance
    - Audit
    - Recommended Standards

Security – First Steps

Table of Contents

Security – First Steps

Key Points

To implement security effectively, you need a balanced approach that covers your staff, your administrative processes and your technology. This section deals with the fundamental first steps:

- Set up a security program that takes a comprehensive approach to your physical, technological and administrative operations.
- Assess your current security situation to determine your priorities and serve as a baseline for the program.
- Develop a security policy that commits the organization to appropriate security measures and provides high-level direction on how this will happen.
- Develop an appropriate set of security standards and procedures based on your policy.
- Appoint a staff member with overall responsibility for security.
- Define, document and communicate the responsibilities of this role and all the other roles required to support your security policy.

Documents you should create as a result of carrying out these steps include:

- Security Policy, Standards and Procedures
- Initial Security Review Results
- Personal Health Information Inventory (Appendix B)

Security Program and Policy

You must take reasonable steps to keep personal health information secure. What is reasonable may vary depending on your organization's size and complexity, and the nature and extent of risks faced within the organization. Large hospitals dealing with significant amounts of sensitive personal health information that have internal networks, centrally managed IT and many staff members accessing information electronically will need different security than small offices. You must decide where your organization falls on the range between large institution and small office. Scale your measures to a reasonable level that fits your circumstances.

What You Should Do

Set up a security program that takes a comprehensive approach to your physical, technological and administrative operations.

Assess your current security situation to determine your priorities and serve as a baseline for the program.

Develop a security policy that commits the organization to appropriate security measures and provides high-level direction on how this will happen.

Develop an appropriate set of security standards and procedures based on your policy.

Your security program must be comprehensive because good security does not rely only on a strong lock on the front door. Good security relies on a series of measures in place just in case the lock gets broken or the back door is left open. Your program must also cover all security measures and not just technical ones. Installing anti-virus software to secure personal health information is important. But, it is not enough. Security is easily breached by simple mistakes such as sensitive information being left lying around or a wrong number being punched in when faxing a patient record.

You need to make an initial assessment of your current security situation to determine the critical areas you must address first and also to set the baseline you will measure against to determine the effectiveness of your security program. This assessment should analyze both your current security risks and controls. If

you don't have the skills within your institution to do this, seek outside help to do the assessment properly since it will serve as the foundation for your program.

A written security policy is important as it will guide your staff on overall security matters and provide a base for creating specific standards and procedures. Your initial security assessment will provide input to help you build the policy that best meets your security needs. You also need to have a good understanding of your legal, regulatory, ethical and contractual security obligations in order to build your policy.

At a minimum, the highest levels of your management should approve your security policy. Your security policy should include:

- what security means to your institution and why it is so important,
- key security goals and principles,
- individuals' basic security responsibilities and accountability,
- how staff will be trained,
- who will review and update your policy, and
- how you will comply with your contractual and legal security obligations.

You should use your policy to help develop a fully documented set of security standards (for example, password rules) and security procedures covering both:

- how you protect your perimeter (such as the main entry point to your building or computer network), and
- what occurs inside your building or network (because your employees are not free to see any information they want, nor are they immune from mistakes or bad judgement).

The security policy should integrate with other policies, particularly privacy.

Tell your staff and outside contractors about the policy.

Small Office Applicability

- Give your staff a concise written set of security rules that also explain why the rules must be followed.
- Remember that everyone must play their part in protecting your patients' personal health information and your facilities.

- The Small Office Applicability sub-sections in this section will help you customize rules that fit your office.

Roles and Responsibilities

What You Should Do

Appoint a staff member with overall responsibility for security.

Define, document and communicate the responsibilities of this role and all the other roles required to support your security policy.

- Assign at least one staff member (for example, the Security Officer) overall responsibility for security. See Appendix A for a sample of this person's responsibilities.
- Establish a cross-functional team of senior managers to review security status, requirements and direction and ensure security issues are addressed with long-term solutions. The team should meet regularly.
- Consider appointing a Data Steward to define the exact policies for access to stores of personal health information.
- Appoint one staff member in each critical process (such as transferring health records) to be responsible for that security process. This role differs from the Data Steward role as the latter deals with disaster recovery requirements rather than specific data-handling requirements.
- Define, document and communicate security responsibilities for personnel managers, general employees, and those with security roles for specific processes.
- Define specific security duties for employees responsible for maintaining security controls and with special access for technical support.
- Ensure security through "separation of duties." Individuals should neither audit their own performance nor authorize their own access to a system.

- If security responsibilities can be delegated, for example, where a Data Steward may appoint someone to perform day-to-day data access approvals, define the delegation precisely.
- Do not delegate responsibility for determining security requirements to third parties. Define security requirements in any contract with third parties with access to personal health information. Build in appropriate monitoring measures to ensure they comply.
- Your list of security responsibilities should cover specific security incident response procedures (such as responding to security breaches).

Small Office Applicability

- The law makes physicians ultimately responsible for security.
- While all staff play a role, the buck stops with the custodian of personal health information.
- Make clear to your staff what are their security responsibilities (as described in other sections of this Toolkit). Train staff on these responsibilities when hired. Ask them to sign that they understand and will abide by their responsibilities.

Information Inventory and Classification

What You Should Do

Maintain a categorized inventory of all your stores of personal health information.

- List all stores of personal health information. Capture the essential facts about the information and how it should be handled. (A sample Inventory Template is included in Appendix B).
- The inventory should include all formats and media used to store personal health information including electronic, hardcopy, microfiche, audiovisual media, photographs and other images.

Security – First Steps

- Build your security policy around a data classification scheme. Categorize the types of information you collect and store and define security controls for each category. Typical categories include:
  - **public** – no restrictions,
  - **internal** – for use inside the institution only,
  - **confidential** – for use only on a "need to know" basis, and
  - **restricted** – controlled access to specified individuals.
- All personal health information should be classified as at least confidential.

Small Office Applicability

- Keep accurate records of the personal health information you store. Include both hardcopy and electronic information and information that may be outside your office.
- Implement appropriate security measures to protect the information. At a minimum, store hardcopy information under lock and key and protect electronic information by password.

Checklists, Templates and Tools

Appendix A – "Roles and Responsibilities" provides a sample of a Security Officer's Responsibilities

Appendix B – "Information Inventory and Classification" provides a sample Information Inventory Template

APPENDIX A – ROLES AND RESPONSIBILITIES

Sample Security Officer Responsibilities

- Setting, reviewing and updating security policy.
- Ensuring staff and contractors are aware of the policy and informed on how they should support it.
- Driving implementation of supporting procedures and controls.
- Ensuring security controls are audited.
- Conducting Threat Risk Assessments (TRA) for any changes to processes or IT systems that could affect security. (See sample TRA form in Sustaining Security section.)
- Investigating security incidents and ensuring long-term solutions are in place. (Security incidents occur whenever your security controls are compromised or challenged beyond any thresholds you have set. If the incident compromises personal health information, it also raises privacy issues; you should follow the guidelines in the Oversight section of this Toolkit to manage a privacy breach.)
- Developing a close working relationship with the contact person or equivalent (since these roles are intimately connected).
- Advising staff and contractors on security.

APPENDIX B – INFORMATION INVENTORY AND CLASSIFICATION

Sample Information Inventory Template

Create and maintain a high-level inventory of all the computer and hardcopy stores of personal health information you have. Remove the sample information and customize the table according to your needs.

Name	Information Types	Info Steward	Location	Backup Copies	Security	Retention
Master Patient Health Records	Patient info: - Name - Contact info - Health # - Family info - Health history	John Q. Deere	UNIX server at College Street location	Offsite storage facility in Markham	Confidential: password-protected via EHR application on encrypted in storage	Archive after patient inactive for • years
MRI Records	MRI images with: -patient name -health # -date	Jane P. Doe	MRI Cabinet, 4th floor, University Avenue	None	Confidential: Locked cabinet (key with Jane) Sign-out sheet for borrowing records	Destroy after patient inactive • years

Storage requirements should include any special measures needed for the type of media used, such as limits on heat, humidity, ultra-violet light and magnetic fields.

Security – People

Table of Contents

Security – People

Key Points

Your security is only as strong as your staff. Even the best technological security is vulnerable if you do not have staff committed to safeguard confidential information. This section deals with the steps needed to address the people aspect of security:

- Inform and motivate all staff and contractors. Give them the necessary tools to carry out their personal security responsibilities. Training should include awareness and commitment to:
  - Security Policy
  - Malicious Software Rules
  - Responsibilities for Physical Security
  - Acceptable Use Policy
  - Rules for Fax Machines
  - Confidentiality Agreement
  - Password Policy
  - Guidelines for Mobile Computing
  - Incident Reporting Rules
- Impose controls to ensure no one gains access to personal health information without proper authorization.

Documents you should create as a result of carrying out these steps include:

- Staff Responsibilities for Physical Security (Appendix A)
- Acceptable Use Policy and Rules for Fax Machines (Appendix A)
- User ID and Access Management Procedures (Appendix B)
- Password Policy (Appendix B)

Personal Responsibilities for Security

What You Should Do

Inform and motivate all staff and contractors. Give them the necessary tools to carry out their personal security responsibilities.

- Run appropriate background checks before hiring staff who:
  - deal with personal health information,
  - work on IT infrastructure, and
  - have special security responsibilities.
- Staff should sign confidentiality agreements.
  - Have staff sign the agreement when they are hired and initial their pledge annually as a reminder. Use this as an annual opportunity to reinforce training on privacy and security and brief staff on recent changes.
- All third-party contractors (for instance, consultants) and key contractor staff who may have access to sensitive information should sign an agreement before they begin work.

Physical Security

- Your staff must:
  - be aware of physical security responsibilities,
  - lock up sensitive material,
  - wear identity badges,
  - secure information outside the normal work area, and
  - report suspected incidents.

- See Appendix A for more detailed guidance on physical security and use of fax machines.
- Tell staff what they need to do for on-line security. Issue an "Acceptable Use" policy (see Appendix A for a sample).
- Provide staff with necessary security tools (such as anti-virus software and laptop computer cable locks).
- Create an ongoing security awareness and training program, reinforced with regular updates.

Small Office Applicability

- Lock up hardcopy personal health information if left unattended. Assign someone the task of making sure the office, all personal health information and computers are locked at the end of each day.
- Set power-on passwords on all computers. Install locking screen savers and instruct staff to use the screen saver whenever they leave their computer. Set the screen saver to automatically kick in when the computer is idle for a reasonable period of time.
- Use your computers' built-in security features, such as power-on and hard-drive passwords.
- Make sure staff understand that they should not install any unauthorized software or connect any unauthorized devices to their computers, or use their computers for unauthorized purposes.
- Make sure staff understand that they may not copy or transmit any information from their computers unless authorized. This includes using email or instant messaging.
- Avoid accidental exposure of personal health information, like the "reader over the shoulder" or the neighbour who overhears loud conversations.
- Give staff facilities (for example, shredding machines) to securely dispose of personal health information no longer required.

Authentication and Authorization

Although the following guidelines focus on computer systems, many apply equally to voicemail and hardcopy records.

What You Should Do

Impose controls to ensure no one gains access to personal health information without proper authorization.

- Authentication establishes someone's identity.
- Authorization establishes what someone may do.

Restrict access to all personal health information to only those who "need to know". Give access only to people whose job requires access.

Always provide only the minimum access needed to perform the job.

- Where possible, use two-factor authentication to grant access to personal health information. This requires users to (1) know something, like a password, and (2) have something, like an ID badge. This is especially important when providing remote electronic access to personal health information.
- Implement effective password policies and practices, including standards on password choice, protection and updating. (A sample password policy is found in Appendix B.)
- Avoid shared User IDs so you can hold all individuals accountable for their use of computer and network resources.
- Manage User IDs and associated access rights from issuance through deletion. Appendix B provides details on the practices you should adopt, including:
  - periodically checking to see that User IDs are still needed, and
  - creating special measures for User IDs with access overrides, such as those technical support staff use.

Small Office Applicability

- Provide staff with their own computers, User IDs and passwords, where possible. At a minimum, staff should have their own User IDs and passwords to access personal health information.
- Remove or change access as soon as staff leave or change responsibilities.
- Instruct your staff to create passwords that are hard to guess. Tell them not to write passwords down and, if they must, to store the paper someplace secure. (Recommend passwords at least 8 characters long containing both numbers and letters.) Ask them to change these passwords periodically and never re-use old ones.
- Instruct your staff never to share their passwords except for temporary authorized backups. Passwords should be reset immediately afterwards.

Related Sections of the Act

2, 3, 4, 10, 12, 13, 14, 42, 53

Checklists, Templates and Tools

Appendix A – "Personal Responsibilities for Security" provides a sample List of Staff Responsibilities for Physical Security, a sample Acceptable Use policy and guidance on using fax machines.

Appendix B – "Authentication and Authorization" provides a sample password policy.

APPENDIX A – PERSONAL RESPONSIBILITIES FOR SECURITY

Sample List of Staff Responsibilities for Physical Security

- Lock cabinets and secure removable computing devices such as laptops.
- Follow "clean desk" practices especially in unattended workspaces.
- Wear identity badges, challenge "tail-gaters" entering restricted areas, and sign-in and escort visitors in restricted areas.
- Secure information and computers used outside the normal work environment (for example, in a home office or while tele-commuting or travelling for business).
- Avoid accidentally exposing information, for example, allowing a computer screen to be viewed or a conversation to be overheard.
- Dispose of hardcopy personal health information properly (for example, using a shredding machine). Disposal methods such as shredding machines should meet security standards.
- Properly dispose of digital media by either physical destruction (for example, shredding CDs) or by first erasing information in an approved manner.

Sample Acceptable Use Policy

Modify the following sample policy to suit your requirements. Review with your lawyers before publishing.

- **Applicability**
  - All users, including full- and part-time employees, contractors, temps, affiliates, consultants, and interns, of **[Insert Your Organization's Name]** IT resources are subject to this Acceptable Use Policy.
- **Business Use**
  - Use **[Insert Your Organization's Name]**'s resources exclusively to conduct **[Insert Your Organization's Name]** business or for other uses management authorizes.
  - The following statement (or equivalent statements) must be presented to individuals logging onto **[Insert Your Organization's Name]**

systems during the identification and authentication process if the **[Insert Your Organization's Name]** system is running an operating system that can provide notification (otherwise labels containing the text should be placed visibly at the user interface):

- Use is subject to audit at any time by **[Insert Your Organization's Name]** management. **[Insert Your Organization's Name]** may from time to time monitor use of its IT resources, including email and the Internet, to ensure business use or to investigate suspected problems. Users are advised of this practice before being permitted access to **[Insert Your Organization's Name]** IT resources.

- **Personal Use of Computing Equipment**

  - Only **[Insert Your Organization's Name]** management may approve personal use of **[Insert Your Organization's Name]** computing equipment (if the use is clearly insignificant and complies with **[Insert Your Organization's Name]'**s Business Conduct Guidelines). Personal use may not be approved if it:

    - interferes or competes with **[Insert Your Organization's Name]** business,
    - interferes with any employee's job performance,
    - involves any additional costs to **[Insert Your Organization's Name]**,
    - involves commercial solicitation,
    - divulges company information to others, or
    - involves commercial or personal distribution lists.

  - Questions concerning personal use of **[Insert Your Organization's Name]** computing resources and Internet services should be discussed with the employee's manager.

  - Incidental or infrequent personal use of **[Insert Your Organization's Name]**'s e-mail systems and access to the Internet for personal use may be allowed without management approval provided none of the above prohibitions are violated.

Security – People

- **Instant Messaging**
  - Internal Instant Messaging is subject to all **[Insert Your Organization's Name]** Acceptable Use standards and is subject to the same policies and standards as e-mail communications.
  - External or public Instant Messaging software and services may not be used on any **[Insert Your Organization's Name]** machines or from within the **[Insert Your Organization's Name]** network.
  - Only the authorized **[Insert Your Organization's Name]** Instant Messaging solution may be used.
- **Cell Phones**
  - Cell Phones should not be used to store or transmit confidential information.
  - Use of cell phone cameras is prohibited within **[Insert Your Organization's Name]**.
- **Wireless Network Access**
  - Management must approve in writing all Wireless Access Points. A Risk Assessment must be performed prior to their implementation.
  - Only **[Insert Your Organization's Name]** approved and installed Wireless technology is permitted on an **[Insert Your Organization's Name]** machine or within **[Insert Your Organization's Name]**.
- **Chain Letters, Hoaxes and Virus Warnings**
  - Using **[Insert Your Organization's Name]** computer systems to send, forward or reply to chain letters, free offers, hoaxes or virus warnings is prohibited.
  - Should you receive an e-mail notice about a supposed virus or harmful code threat, notify the Help Desk or check the **[Insert Your Organization's Name]** intranet site.

- **Offensive and Inappropriate Material**
  - **[Insert Your Organization's Name]** employees may neither access nor distribute any material that could be considered inappropriate, offensive or disrespectful to others. Examples include material that:
    - contains sexually explicit images or descriptions,
    - advocates illegal activity, or
    - advocates intolerance for others.
  - Employees should obtain company directives from their managers.
- **Internet Use**
  - These rules apply to both the Internet and internal **[Insert Your Organization's Name]** intranet network.
  - Unprotected information posted on the Internet is available to countless unknown people worldwide, not all of whom support **[Insert Your Organization's Name]**.
  - **[Insert Your Organization's Name]**'s information, computing assets, and corporate image on the Internet must be rigorously safeguarded from loss, modification or destruction.
  - Using the **[Insert Your Organization's Name]**'s Internet access is regulated by policy. Any infringement can result in disciplinary action up to and including termination. Prohibited uses can include:
    - viewing or posting any material considered inappropriate, offensive or disrespectful to others,
    - using unauthorized file exchange or sharing of services (such as Napster, Gnutella, WinMX, LimeWire, BearShare, Morpheus and Kazaa),
    - trading securities,
    - gambling on-line or entering prize competitions,
    - downloading entertainment software or games or playing games, and

    - uploading software or data owned by or licensed to **[Insert Your Organization's Name]** without appropriate authorization.

  - **[Insert Your Organization's Name]** may block access from within our networks to any sites we determine are inappropriate for any reason. If you find yourself connected incidentally to a site that contains inappropriate material, you must disconnect from the site immediately.

  - Posting information about **[Insert Your Organization's Name]**'s employees, vendors, suppliers or partners without a valid business justification is prohibited. Posting personal opinions about **[Insert Your Organization's Name]**'s staff or affiliates is prohibited.

  - Revealing confidential or personal health information, and any other material on chat rooms is prohibited.

  - Downloading infected, unlicensed or unregistered software is prohibited.

- **Electronic Mail**

  - Electronic mail (e-mail) is a business tool that should be used with the same considerations for quality and appropriateness as any other business communication.

  - E-mail is the property of **[Insert Your Organization's Name]** and may be monitored or audited at any time to ensure compliance with Security Policies and Standards or for other reasons at management's discretion.

  - Employees may not represent themselves as someone or something they are not.

  - Sending, creating or storing offensive or disruptive material using email is strictly prohibited. Violating **[Insert Your Organization's Name]**'s business conduct guideline is also prohibited. Prohibited content includes, but is not limited to, racial or ethnic slurs, profanity, and messages containing sexually explicit language or graphics.

  - Any communication using **[Insert Your Organization's Name]**'s e-mail or Internet systems could be construed as representing **[Insert Your Organization's Name]**'s corporate position. Only duly

authorized individuals may speak or write on **[Insert Your Organization's Name]**'s behalf.

- Users must never attempt to gain access to another user's email messages without permission.

- Critical information should not be stored in email.

- **Representation of [Insert Your Organization's Name] using IT facilities (such as email or the Internet)**

  - Employees representing **[Insert Your Organization's Name]** must identify themselves accurately and completely (including their position and function where requested).

  - Any false representation of authority or engagement in unauthorized business is strictly prohibited.

  - Only duly authorized employees or officials may represent **[Insert Your Organization's Name]** and its policies in speech or writing to the media, analysts, or at public gatherings. Other employees may participate in newsgroups or chats in the course of business, when relevant to their duties, as individuals speaking only for themselves. Individuals participating who are identified as an **[Insert Your Organization's Name]** employee or agent must refrain from any unauthorized political advocacy, endorsement or apparent endorsement by **[Insert Your Organization's Name]** of any commercial product or service.

  - Electronic mail addresses may satisfy the requirement for a legal signature. Employees must avoid creating unwarranted contractual obligations. Where the possibility exists, a disclaimer must be included, indicating that official approval must be obtained before agreement.

  - **[Insert Your Organization's Name]** does not accept responsibility for the personal opinions its Internet users express. **[Insert Your Organization's Name]** does not act as a publisher; it simply allows the means to distribute statements its employees make. Employees with Internet access must understand how Canadian intellectual property, defamation and criminal laws may expose **[Insert Your Organization's Name]** to legal liability.

Security – People

- **Compliance With Legal, Statutory and Regulatory Requirements**
  - **[Insert Your Organization's Name]**'s facilities and computing resources must not be knowingly used to violate the laws of Canada or Ontario or of any other jurisdiction in any material way. Using institutional resources for illegal activity is grounds for immediate dismissal, and **[Insert Your Organization's Name]** will cooperate with any legitimate law enforcement activity.
  - Any software or files downloaded via the Internet into the **[Insert Your Organization's Name]** network become the **[Insert Your Organization's Name]**'s property. These files or software may be used only in ways consistent with their licences or copyrights.
  - No employee may knowingly use **[Insert Your Organization's Name]** facilities to download or distribute pirated software or data.
- **Malicious and Damaging Activities**
  - Employees must never use **[Insert Your Organization's Name]**'s Internet facilities to propagate any virus, worm, Trojan Horse or trap door program code.
  - Employees must never use **[Insert Your Organization's Name]**'s Internet facilities to disable or overload any computer system or network, or circumvent any system intended to protect another user's privacy or security. Employees also must never use **[Insert Your Organization's Name]**'s computing resources to gain unauthorized access to remote systems. Any attempts to do so will be reported to the remote systems' administrators and law enforcement personnel where warranted. Deleting, examining, copying or modifying other users' or entities' data or files without their consent is prohibited.
  - Employees must never run security-testing tools or programs against any Internet system or server.
  - Employees must never knowingly write or run any computer program or process (including email) that would consume more computer resources than needed to perform **[Insert Your Organization's Name]**'s work.
  - Employees must not use **[Insert Your Organization's Name]**'s network to perform an Internet transaction that may consume significant system resources and interrupt or delay system use.

Information Technology management must approve any repetitive or large data transactions.

Rules for Transmitting Personal Health Information using Fax Machines

- Transmit personal health information by fax only when no more secure practical alternative exists.
- When you do need to send a fax, always remove common identifiers, such as a patient's name and address (an ID number may be all that is required) from personal health information.
- Because the fax machine receiving your transmission may not be located in a secure area, always let your recipients know that you are about to fax sensitive material to them and confirm their fax number.
- Always include a cover page with your name, telephone number, date and number of pages sent.
- Carefully enter the fax number to ensure you do not misdirect the message and seriously breach someone's privacy.
- To avoid manual keying errors to routine destinations, use the fax machine's auto-dial features, if available.
- Confirm that the intended recipient has received all pages you sent.
- Immediately try to recapture any misdirected fax, and follow the guidelines in this Toolkit for handling a privacy breach if appropriate.

APPENDIX B – AUTHENTICATION AND AUTHORIZATION

Sample User ID and Access Management Practices

- Manage user IDs and access rights.
  - Appoint one person to approve user ID set-up and periodically review that access is required.
  - Make sure users immediately change temporary passwords to a password only they know when they first log on. Never issue temporary passwords that are easy to guess (like "welcome").
  - Transmit passwords securely and separately from information that identifies the user.
  - Immediately remove access when people leave or change jobs.
  - Never reuse old User IDs.
  - Use Identity Management software to manage this process where possible.
- Implement "need to know" access.
  - Give access only to those people whose jobs require access. (For example, those caring for or treating a patient would need to know the personal health information relating to their role in the patient's current primary care and treatment.)
  - Restrict access by the specific fields and range of records each person needs access to do the job. If the technology does not allow a fine enough degree of control, modify or replace the technology as soon as possible, using manual controls in the meantime. (This usually requires spot-checking for correct use of information after the fact).
  - Set default access to read-only (view), and add only where the job function requires more.
  - As the type of access needed increases, the level of approval should increase.

- Always consider whether the job can be performed effectively with either anonymous rather than personal information.
- Build access rules in terms of defined job roles, such as “emergency room physician” or “acute care nurse,” instead of evaluating individual requests.
- Consider other methods to support “need to know” access, such as:

Relationship Based Access Control	Location/ Method Based Access Control	Time Based Access Control
		
User has a particular relationship with the patient before access is granted, (e.g., attending physician)	Access may be denied if the request comes from an insecure location or method (e.g., no access from home)	Access is given only for specific times (e.g., no after hours access)

- Users with special support User IDs that provide more powerful access capabilities should:
  - have a regular User ID for when not performing support functions,
  - not have special IDs in both production and test/development environments, and
  - not have access to delete or modify audit logs.
- Systems should lock User IDs automatically after three failed logon attempts in a row and these events should be logged.

Sample Password Policy

Modify the following Password Policy to suit your environment and requirements, automating as many of the rules as possible.

Security – People

- Password Protection
  - Do not transmit user passwords in clear text form over the Internet, public networks or wireless devices. Passwords generated for an individual user must be conveyed to the user in a secure manner, such as in a telephone or face-to-face conversation, password-protected voicemail box or encrypted electronic mail, or by separating the password from its context (user ID).
  - A new password may be generated only after the system administrator or designated authority has positively identified the user.
  - When temporary passwords are issued for new or reset User IDs, the user should immediately change to a password no one else knows when first logging on.
  - Change default user IDs with default passwords shipped with operating systems and program products for use during system and product installation and set up as soon as possible during or following their initial use.
  - If possible, user passwords must be encrypted when stored in files or databases on systems and servers. If passwords cannot be encrypted, access to the file or database element containing the passwords must be restricted to only authorized system security administrators. If passwords are not encrypted during storage and transmission, they may be hashed with a one-way function. Hashing with a one-way function is considered acceptable protection for passwords when transmitted across a network.
  - Do not disclose to or share with anyone your password, including administrative assistants or secretaries, unless individual accountability can be maintained.
  - User password management is a condition of your employment.
  - Do not write your password down. If this is unavoidable and you must write it down, protect the writing containing your password as confidential information, keeping it in your possession or under lock and key at all times.
  - Do not store passwords in a file on any computer system (including Palm Pilots or similar devices) without strong encryption.

- Passwords must never be included in any automated log-on process (for example, stored in a macro or function key) or plain-text batch files residing on a user's local workstation to hasten log on without having to key the user-ID/password combination in.

- Close or log out of password protected web sessions as soon as you have finished with them.

- Password files for a system must be separated from other system and application data, and should never be available to non-administrative users.

- Passwords for critical systems and network components must be sealed and stored in a physically secured location to permit emergency use by designated personnel when necessary.

- Do not possess nor use any tool that would obtain, disclose or capture another user's password.

- Controls must be in place to prevent an unlimited number of invalid logon password attempts (like password hacking). This will be accomplished by either revoking or locking the user ID on the fourth consecutive invalid attempt or using a logon inductor to exponentially increase the amount of time between sign-on screens (to prevent automated tool password hacking).

- Passwords must be changed regularly (monthly or quarterly). Old passwords should not be re-used.

- If an account or password is suspected to have been compromised, report the incident and change all passwords.

- All unsuccessful authentication attempts will be logged.

- The Information Security Department or its delegates will perform password cracking or guessing periodically or randomly. If a password is compromised during one of these scans, the user will be required to change it.

- Password "Don'ts":

    - Never reveal your password to anyone including your manager, family members and co-workers, except as part of an authorized password management process.

- Never discuss your password in front of others or hint at your password's composition (for example, "my family name").
- Never reveal a password on questionnaires or security forms.
- Never use the "Remember Password" feature on applications (for example, Internet Explorer, Eudora, Outlook, Netscape Messenger).

- Password-cracking programs can break weak passwords in minutes. Observe these rules to build strong passwords.
  - Passwords should be at least 8 characters long.
  - Passwords should contain a mixture of letters, numbers and special characters (for example ! @ # $ %), if possible.
  - Avoid dictionary words within the password.
  - Avoid using passwords based on easily guessed ideas, such as birth dates, family or pet names, hobbies, sports or months.
  - Avoid keyboard sequences (for example QWERTY) and logical sequences (for example, ABC, 1-2-3, zyx, 10-9-8).
  - Avoid repetitive sequences (a number or letter used more than twice).
  - Do not use the same password for work and non-work User IDs (for example, personal ISP account, option trading, benefits, etc.). Avoid using the same password for multiple work User IDs.
  - Do not re-use old passwords.
  - Temporary passwords for new or reset User IDs should not be re-used (generate a new one for each situation) and should not be easy to guess (for example "welcome").

Security – Institutional Safeguards

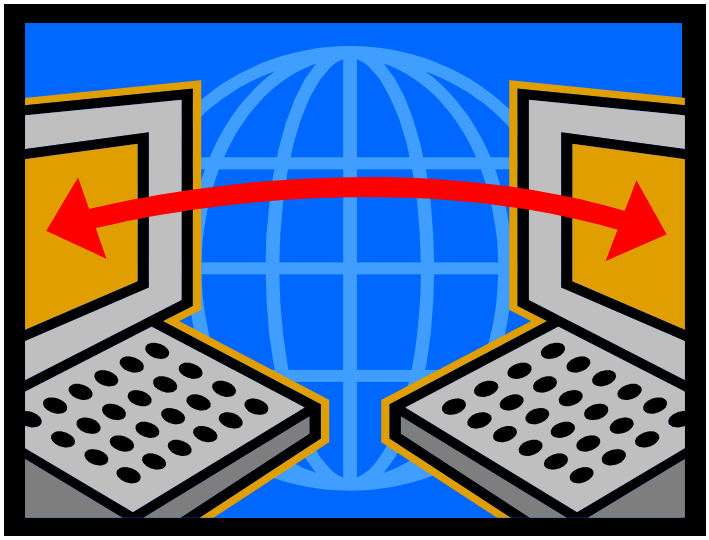


Table of Contents

Security – Institutional Safeguards

Key Points

To implement security effectively, you need a balanced approach that covers your staff, your administrative processes and your technology. This section deals with the steps needed to secure the institution. These steps have some implications for general users but would largely be carried out by IT professionals:

- Secure the physical and electronic (computer) points that provide access to personal health information.
- Use appropriate measures to protect information technology from malicious software.
- Implement an incident response plan to address any incidents that do occur.
- Put policies and procedures in place to reduce the security risks associated with wireless and portable devices.

Documents you should create as a result of carrying out these steps include:

- Malicious Software Policy (Appendix B)
- Malicious Software Guide (Appendix B)
- User Guidelines for Mobile Computing (Appendix C)
- An Incident Response Plan
- A Plan to Manage Computer or Digital Media Theft or Loss (Appendix A)

Perimeter Security

What You Should Do

Secure the physical and electronic (computer) points that provide access to personal health information.

Physical Perimeter Security

- Lock printed files and removable storage media (CDs etc.) containing personal health information in secure places.
- Use physical entry barriers to restrict access to personal health information to identified and authorized personnel. Examples include:
  - active supervision by a security guard or receptionist, or requiring visitors to sign-in, and
  - passive control through an automated security badge system, surveillance cameras or alarms.
- When printed health records are used outside the controlled area:
  - use a sign-out log to record who borrows the record,
  - tell them how the record is secured, and
  - check the sign-out log at the end of each day to ensure all records due back have been returned.
- Supervise third-party access (for example, cleaners, building security and landlords) to areas where personal health information is kept.
- Monitor printers and fax machines for documents containing personal health information or keep these devices in rooms with restricted access.
- Remove or encrypt any personal health information from computer equipment sent off-site for maintenance. Ensure those who service your equipment sign an agreement as well (see the Managing Contracts and Agents section).

- Use secure medical courier delivery services wherever possible for transporting personal health information.
- Use sealed containers to transport personal health information between secure facilities. Consider using packaging that reveals when it has been tampered with and check that quantities sent and received match.
- Secure centrally managed computing equipment and network cabling to prevent tampering or unauthorized connection of other devices.

Electronic Access Points

- Use network security measures, such as firewalls, to stop unauthorized traffic from entering your computer network.
- Segregate the network into different security zones to provide more protection for information that needs it. See Appendix A for details on Security Zones of Control.
- Use secure remote access methods, such as Virtual Private Networks (VPNs), to provide authorized users with secure remote access to your institution's network.

  Note: VPNs refers to technology that allows authorized users to send information over a public network, like the Internet, in a protected manner with safeguards equivalent to that of using the organization's private network.

- Do not tolerate unmanaged network access points (for example user-connected dial-up modems or wireless hubs).
- Erase or destroy personal health information stored on computer equipment when selling or disposing of the equipment. (Just using the "delete" or "format" function is often not good enough; you may need to destructively erase the storage devices, such as using a magnetic eraser, so the information cannot be recovered).

Small Office Applicability

- Keep physical files containing personal health information in an area that is locked and supervised when not locked.
- Watch printers and fax machines when in use or keep them in a locked area.

- Run up-to-date Personal Firewall software on all computers in your office that store personal health information.
- Destroy or destructively erase the storage devices on your computers when selling or disposing of the computer (just using the "delete" or "format" function is often not good enough).
- Make sure personal health information is not exposed when your equipment is serviced. Remove or encrypt any information that is not protected by a hard drive password when equipment goes off-site and have those servicing your equipment sign an agreement (see the Managing Contracts and Agents section).

Malicious Software

What You Should Do

Use appropriate measures to protect information technology from malicious software.

Implement an incident response plan to address any incidents that do occur.

Malicious software is designed to damage, break, overtake or steal information from your computers. It includes viruses, worms, Trojan Horses, logic bombs and spyware. Personal computers are especially vulnerable since most malicious software targets them directly. Protecting personal computers is vital.

- Implement a malicious software policy and provide simple rules for your staff to follow (See Appendix B for a sample policy and user guide).
- Develop an incident response plan to combat any malicious software attacks. Appoint one staff member to:
  - co-ordinate your response,
  - assess the incident's severity and scope,
  - identify the best way to address the incident,
  - tell staff what to do,

  - implement a business continuity plan to restore lost facilities, programs and data, and
  - implement long-term solutions.

- Track and implement any applicable updates software vendors develop to fix known security problems with their software.
- Larger institutions should consider workstation management software or services that automatically send vendors' fixes to all users.

Small Office Applicability

- Run up-to-date Anti-Virus, Firewall and Spyware software on all computers that store personal health information.
- Use the associated update service to ensure your software can catch the latest known viruses.

Wireless and Portable Devices

What You Should Do

Put policies and procedures in place to reduce the security risks associated with wireless and portable devices.

Portable devices include Laptop Computers, Personal Digital Assistants and Cell Phones.

- Do not use wireless devices (such as email or cell phones) to transmit personal health information unless the system is designed to support wireless devices securely (for example, with data encryption).
- Do not use portable devices to store personal health information, except systems designed to support portable devices securely.
- Instruct staff using portable devices outside of the secure work area to take precautions against theft and unauthorized access. Remind them that the "reader over the shoulder" is a real risk.

- If you do not have the skills on staff, get an IT security professional to help design and implement your wireless systems securely.

Small Office Applicability

- Assume wireless and portable devices are not secure unless you had a security professional set them up to be secure.
- Do not use wireless and portable devices to store or transmit personal health information. Cell phones are not secure and you need to be careful when deciding what information to discuss on a cell phone (use a regular phone whenever possible).

Related Sections of the Act

2, 3, 4, 10, 12, 13, 14, 42, 53

Checklists, Templates and Tools

Appendix A – "Perimeter Security" provides guidance on Security Zones of Control, LAN Management and Managing Computer Theft

Appendix B – "Malicious Software" provides a sample policy on malicious software and a sample guide for users

Appendix C – "Wireless and Portable Devices" provides a sample user guide and sample technical standards

APPENDIX A – PERIMETER SECURITY

Network Design – Security Zones of Control

The concept of security zones is most applicable to large institutions with complex networks serving many different types of user including the public and external suppliers. A security zone is an area where a defined set of security policies and measures combine to achieve a specific level of security. In a large networked environment it is usually better to define multiple zones that group computing resources with similar security requirements and cluster levels of risk together. Specific security mechanisms and policies outline the criteria that should be met to transit from one zone to another. Separating the zones ensures that security failures in less secure zones do not compromise more secure zones. Large organizations typically use the following zones.

A *Highly Secure Zone* is used to store or process sensitive, private or confidential information. Access is strictly limited to identified entities. Very stringent security mechanisms protect the Highly Secure Zone. User credential information (password files) and highly sensitive personal health information typically belong in the Highly Secure Zone. Any information requiring the highest confidentiality, integrity or availability should be considered for this zone.

An *Internal Zone* is used for storing and processing sensitive, private or confidential information. Security policies are strictly enforced, but access need not be as restricted as in the Highly Secure Zone. The Internal Zone includes the network, applications and facilities implemented to support internal systems. It also includes internal systems outsourced to external partners, but does not include systems that act as access points-of-entry for those partners.

The Internal Zone is subdivided into *Security Sub-Domains*. In general, a sub-domain is a logical boundary separating a collection of resources that must be separated from the rest of the security zones for some special purpose, but are still considered part of the larger zone. These sub-domains should not weaken the larger zone and may require additional security controls to isolate them from the common infrastructure. Note that Sub-Domains should be exceptions and limited in number.

A *Buffer Zone* (Internal Controlled) houses applications and services provided to give entities in the Public or External Business Zone access to less-sensitive resources. Security controls are applied at the Buffer Zone's entry points and between the Buffer and Internal Zones. No direct connection between the Public/External Business Zones and the Internal Zone is allowed (meaning all connections to the Internal Zone should be via the Buffer Zone).

External Business Zone (External Controlled) is where information and systems are shared with other institutions, stakeholders and external users. Equivalent security policies and standards are mutually acceptable and verifiable. The External Business Zone generally is another organization's infrastructure that your organization connects to for specified business activities. For instance, a regional hospital might link to local hospitals in this way.

In the *Public Zone* (External Uncontrolled), information and systems are open and uncontrolled. Security policies and standards cannot be enforced. A hospital's public website might represent such a zone.

Guidance For Managing Computer and Digital Media Theft and Loss

Most of the following steps for managing theft or loss should be taken before an incident occurs. Some of the steps address your options following a theft.

- Conduct a regular inventory of all of your IT equipment and assets and ensure sure you have the following information:
  - Owner Name
  - Description (brand, model, and features)
  - Location
  - Serial Number
- Larger institutions should consider using asset management software to inventory software assets on workstations.
- Map assets:
  - that support critical business functions within the Business Continuity Plan, and
  - containing the critical information identified in the Information Inventory and Classification section.
- Put Acceptable Use and other personal security policies in place that require staff to take protective measures, such as:
  - physically locking portable IT assets (including computers, PDA's, and portable media such as hard drives, CDs and USB memory keys) and keeping them hidden from view, and

  - using encryption for sensitive data and employing hard drive passwords.

- Take additional steps for very valuable assets and those containing very sensitive data:
  - Install GPS tracking devices.
  - Use storage devices that over-write data when tampered with.
- Establish a process to manage stolen or missing IT assets.
  - Designate a contact point for reporting stolen assets (such as a Help Desk).
  - Appoint a coordinator to:
- establish how critical the lost or stolen asset is,
  - contact law enforcement or tracking agencies as appropriate, and
  - tell those who may be affected of the asset's loss (see Section on Managing a Privacy Breach).

When an incident occurs, take the following steps:

- Report the incident to police and internal security (providing serial numbers).
- Lock any computer accounts associated with the asset.
- Notify managers of affected departments to stem any wider implications the loss may have.
- Notify your legal department and communications staff if you think any information leak may affect the public or clients so they can decide whether to alert regulators and draft a press statement.
- Review the incident (consider any motive involved and look at similar incidents).
- Consider prosecution if an individual is apprehended or identified.
- Review security practices to determine whether the incident could have been prevented.

Sample LAN Management Guidelines for Large Installations:

LAN stands for Local Area Network

Modify the following guidelines to suit your needs and own local area network.

LAN Management Physical Security

- Treat LAN devices like computers or servers and follow same physical and logical security rules for servers.
  - LAN devices should be house in a secure enclosure accessible to only authorized personnel.
  - Grant access to a LAN device following the same rules and restrictions for physical access to a server.
- Do not expose LAN cables or leave them open to unauthorized access, except at their terminal end when connecting to the user workstation.
  - Wiring closets and patch panels should be locked and accessible to only authorized personnel.
  - Cable runs should not be accessible from public-use areas. If cable runs are accessible, consider using positive-pressure sealed conduits.
- LAN connections should be available only inside internal areas with access restricted to authorized employees.
  - If LAN connections are needed in semi-public areas (like meeting rooms used for visitors or visitors' waiting areas) enable Media Access Control (MAC) address filtering on those ports to accept only connections from known machines. If policy-based networking has been implemented, stronger protections may be deployed.
  - If visitors need a LAN connection, it should be routed to a public network zone in the network (Internet) and not to the internal LAN.
  - Verify and audit physical port counts regularly.

LAN Management Logical Security

- Segment the LAN based on application and data usage. For example, Human Resources data should reside on servers on a different network than patient data.

- Intelligent LAN devices (for instance, large switches and routers) must be protected by passwords the same way and following the same rules as a server. Do not use default or generic passwords.

- Consider using an out-of-band management network to manage networked devices. If direct console access is necessary, use a terminal server with strong authentication options.

- Upgrade LAN devices using control software that can be maintained with patches as required.

    - Treat these LAN devices the same way as a server and apply the same procedures for maintenance and security patches.

    - Maintain strict controls on who may change these devices and keep backup copies of configurations in a separate backup location.

- Do not enable remote access to network devices.

    - If a valid administrative reason requires remote access, treat the access the same way as a server remote access, protecting it in the same way (using digital credentials, smartcard, or similar authentication mechanisms).

- Only authorized computers or servers should connect to the LAN.

    - At a minimum, if a computer or server not controlled by **[Insert Your Organization's Name]** must be connected to the LAN, it should be inspected and verified by **[Insert Your Organization's Name]** personnel to ensure no malicious elements (viruses, Trojan horses, etc.) are hidden in it.

    - For stronger protections, consider policy-based networking, which typically combines authenticating before end-users gain access to the network, enforcing security policies and standards, and verifying that the end-client is patched and up to date.

- No "shares" or folders should be visible or available in the LAN without a proper login using a password that follows **[Insert Your Organization's Name]** password rules.

    - LAN passwords should follow the same rules as other critical passwords and have similar expiry times.

- The protocols used in the LAN environment must be up-to-date and comply with the security policy. Avoid protocols that are obsolete or have known vulnerabilities. (For example, wherever possible, do not use basic SNMP, using common public and private community strings for access. SNMP versions 2 and 3 offer much more suitable authentication and encryption options).

- Dual homing (connecting a computer to two different networks at the same time) is not allowed, unless **[Insert Your Organization's Name]** controls both networks and the networks have identical security controls.

  - Dual homing exists when a single computer is connected to the LAN and another network, such as a wireless one, another LAN, or a dial-up.

- Control all outside access into the LAN from outside and deny access to unauthorized users.

  - Protect all connections to other LANs and the Internet with Firewalls.

  - Deploy Intrusion Detection Systems (IDS) in Internet connection points to detect unauthorized attempts to access the LAN.

  - Enable logging-in LAN devices whenever supported.

  - Archive access logs in a protected server and review them regularly. Review can be automated or manual, but should be at regular intervals. Reports should be generated if any event flags intrusion attempts.

- Disable all unused network ports.

- Disable all unnecessary protocols.

- Use anti-virus software, bandwidth throttling and other Quality-of-Service (QoS) mechanisms to help prevent and impede network-based malicious code from spreading.

Sample LAN Management Guidelines for Small Installations

Modify the following guidelines to suit your environment and your requirements.

LAN Management Physical Security

- Locate LAN hubs or switches out of the general public's reach.

- LAN access ports should not be accessible to the general public.
- Allow only authorized computers to connect to the LAN.

LAN Management Logical Security

- No critical “shares” or folders should be visible or available in the LAN without proper password protection.
- If the LAN is used to access the Internet, use a router with built-in firewall as the main access point.
- No computer should be connected to the LAN and another network (such as a wireless one or a dial-up connection) at the same time.
- Do not use default or generic passwords on networking equipment.

APPENDIX B – MALICIOUS SOFTWARE

Sample Policy for Protecting Against Malicious Software

Modify the following sample policy to suit your environment and your requirements.

- To protect the integrity of software and information, implement precautions to prevent, detect, and cleanse the introduction of malicious software.
- The following controls shall apply to all workstations (business or personal) used for **[Insert Your Organization's Name]** business:
  - A formal policy requiring compliance with software licenses and prohibiting the use of unauthorized software.
  - **[Insert Your Organization's Name]** supplied malicious software detection and repair software must on any workstation used for **[Insert Your Organization's Name]** business or connected to the **[Insert Your Organization's Name]** network.
  - Signature files routinely updated to within the two most recent versions.
  - Anti-virus software activated at boot-up time.
  - If supported by anti-virus software, automatic scanning is enabled.
  - Scanning any floppy or CD-ROM used for the first time.
  - Scanning any files on electronic media of uncertain or unauthorized origin, or files received over un-trusted networks, for viruses before use.
  - Scanning any electronic mail attachments and downloads for malicious software before use. This check may be carried out at different places, for example, at electronic mail servers, desk top computers or when entering the **[Insert Your Organization's Name]**'s network.
  - Employees may download data from known and trusted suppliers after following the virus-checking process and using the approved virus detection package.

- Staff are trained for security awareness, covering the virus protection on systems, training in their use, incident reporting procedures, and recovering from virus attacks

- Appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements.

- Users are instructed not to intentionally write, generate, compile, copy, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any computer's memory, file system or software.

- Computer users are instructed to not knowingly write or run any computer program/process that would consume more computer resources than necessary for performing **[Insert Your Organization's Name]** work.

- Users are aware of the dangers of browser executable code and active scripts

- Browsers' ability to run ActiveX, JavaScript, Java and other forms of active scripts of code are disabled, where feasible.

- Users know to allow executable code and active scripts to be run from only trusted sites.

Sample Malicious Software Guide for Users

Modify the following sample to suit your environment and your requirements.

- Do not remove or alter the anti-virus software installed on your computer and do not shut down its regular scanning activity. Contact the Help Desk if you suspect it is not running correctly.

- If you suspect your computer has a virus, contact the Help Desk immediately, inform you manager and do not use your computer again until you get further instructions from the Help Desk

- Do not respond to any instructions for dealing with viruses that are not from the Help Desk or not posted on our intranet site.

Security – Institutional Safeguards

- Do not send colleagues any instructions for dealing with viruses you receive. The instructions may not be appropriate for them. Our virus response team will handle all communications.
- Beware of unexpected e-mail and e-mail from someone you do not know. Attachments may contain a virus.
- Never use web-based e-mail at the office or download software from the Internet. These files are not scanned for viruses.
- Always scan for viruses files downloaded from the Internet, e-mail attachments, CDs, DVDs, and diskettes.
- Always scan new software for viruses before installing it on your computer.
- As a precaution against a virus attack, make sure your critical files are backed up and retrievable.

APPENDIX C – WIRELESS AND PORTABLE DEVICES

Sample User Guidelines for Mobile Computing

Modify the following guidelines to suit your environment and requirements.

- **Laptop Computer and Travel Security**
  - Always use a cable lock to secure your laptop to your workstation
  - Keep your laptop in your possession as far as possible when travelling.
  - When traveling by air, do not check laptops in as baggage, and be alert to the possibility of theft when going through airport security checkpoints.
  - Never leave your laptop for an extended time in an unoccupied vehicle. If you must leave your laptop in an unoccupied vehicle, ensure it is not visible and secure the laptop to the body of the vehicle inside the trunk with a locking cable.
  - Avoid leaving your laptop in a hotel room. If you must, lock it in the hotel safe or use a locking cable to secure it out of sight in your room.
  - If you are traveling with **[Insert Your organization's Name]** sensitive or confidential material on portable media such as paper, diskettes, notebooks, or other devices, protect this media following the same guidelines listed above for protecting your laptop.
  - Do not work in open public areas where others may view user IDs, passwords, or **[Insert Your organization's Name]** data. (Be especially cautious on airplanes).
  - Never discuss **[Insert Your organization's Name]** confidential information in public areas where you may be overheard, including in conversations on telephones or cell phones.
  - Report the loss of any mobile device containing **[Insert Your organization's Name]** information to the Help Desk immediately.

Security – Institutional Safeguards

- **Security of Handheld Devices**

  - Hand-held devices (such as Personal Digital Assistants, RIM BlackBerry, and mobile phones with data access) storing or accessing **[Insert Your organization's Name]** confidential or business-sensitive data require physical and electronic access controls. The following actions are required:

  - Keep handheld devices in your possession whenever possible.

  - Activate data encryption, power-on password and password-controlled time-out/lock-out features on all hand-held devices supporting these security features.

  - Remote synchronization via modem to move the **[Insert Your organization's Name]** data between the device and your workstation must go through a **[Insert Your organization's Name]** authorized remote access gateway.

- **Wireless/Remote Network Access**

  - Use only **[Insert Your organization's Name]**'s approved remote network access facilities to gain access to the network from outside the office.

  - Ensure that you are not connected to any other network (for example via dial-up modem) at the same time you are connected to the **[Insert Your organization's Name]** network.

  - Never use publicly available wireless networks (often referred to as "hotspots"), unless you (a) have adequate perimeter and antivirus controls and (b) are not transmitting sensitive **[Insert Your organization's Name]** information.

  - Only **[Insert Your organization's Name]** approved and installed Wireless technology is permitted on any **[Insert Your organization's Name]** machine or within **[Insert Your organization's Name]**'s environment. Installation of personal wireless technology into the **[Insert Your organization's Name] environment is considered to be a serious breach of [Insert Your organization's Name]** security policy.

Sample Technical Standards for Wireless Connections

Modify the following sample to suit your environment and requirements.

- Cellular-based wireless is assumed to be public and untrustworthy. **[Insert Your organization's Name]**'s secure remote access mechanisms must be used to access **[Insert Your organization's Name]** resources over cellular-based networks.
- The following standards must be observed for all wireless LANs:
  - Unless explicitly for public-access use only, open wireless LAN networks must not be deployed. If public-access wireless is deployed, it must be adequately isolated from the other parts of the network.
  - Simultaneous wireless and wired connections on the same machine are prohibited.
  - Wireless Access Points must be isolated by firewalls and application proxies.
  - Sensitive applications and data should not be available via wireless connections unless additional layers of security have been added at OSI Layer 2 (WPA, EAP, LEAP, PEAP) and OSI Layer 3 (IPSEC VPN Tunnel).
  - Mitigate basic potential exposures created by the passive interception of wireless network traffic. Some exposures can be mitigated through good wireless network management, including:
    - MAC address filtering must be used to prevent unauthorized clients from connecting through wireless LAN access points. While these addresses can be imitated (spoofed), this does protect against casual attacks and unintentional client associations.
    - Service Set Identifier (SSID) broadcast must be disabled or the beacon interval must be increased to the maximum interval. As these broadcasts can be intercepted, naming conventions (for SSID, status fields, for instance) must not reveal any information (such as department or company name). Default (vendor-supplied) SSIDs are not permitted.
    - Connections from "null" or "any" SSIDs must be denied.
    - Default administrative passwords must be changed to strong passwords. This should include SNMP community strings accessible from the wired side of any Access Point.

    - All unnecessary protocols on the Wireless Access Point must be disabled (including ad hoc networking capability). Adhoc networking (peer-to-peer) must also be disabled on all **[Insert Your Organization's Name]** wireless LAN clients.
    - Management of Wireless Access Points from any wireless interface must be denied. Access Points may only be managed from wired terminals.
    - IP and MAC address filtering must be used to manage Wireless Access Points.
    - SNMP traps must be set on Wireless Access Point resets or configuration reloads.

- 802.11i Wireless LANs must be deployed where possible to provide the highest level of confidentiality and integrity protections currently available. It combines:
    - strong authentication and/or encrypted authentication channels for single-factor encryption, and
    - robust cryptographic services based on the Advanced Encryption Standard (AES).
- If 802.11i is not supported, WiFi Protected Access (WPA) may be used as it provides:
    - the same cryptographic services as standard wireless LANs but with changing keys to help prevent compromise, and
    - strong authentication and/or encrypted authentication channels for single-factor encryption.
- Where 802.11i and WPA are not supported, an exception to this standard must be obtained. At a minimum, these exceptions must:
    - support strong user-based authentication,
    - enable 128-bit (or higher) WEP encryption, and
    - change default WEP keys to a random value and rotate bi-weekly.
- WEP-based protections must be used for home use. At a minimum, 802.11i and WPA Home Edition are strongly recommended (versions not requiring strong authentication are available).

Sustaining Security

Table of Contents

Key Points

To implement security effectively, you need a balanced approach that covers your staff, your administrative processes and your technology. Security is also an ongoing program and not a one-time project. This section deals with the steps needed to sustain security:

- Ensure critical functions can operate and critical data is protected if local disasters or major technology failures cripple your systems.
- Institute policies to ensure security is considered when developing, buying and maintaining IT resources.
- Regularly audit your actual practices for compliance with your security policy.

Documents you should create as a result of carrying out these steps include:

- Data Backup, Disaster Recovery and Business Recovery Plans (Appendix A)
- Guidelines for Secure Applications (Appendix B)
- Any relevant Threat Risk Assessments (Appendix B)
- Security Review, Spot Check and Audit Results
- A Strategy for Capturing and Using Audit Information (Appendix C)

Business Continuity

What You Should Do

Ensure critical functions can operate and critical data is protected if local disasters or major technology failures cripple your systems.

- Analyze the data and critical systems you need to maintain your operations if the technology fails.
  - Identify key personnel for each critical process, such as health records transfer, who can best identify the systems, staff and data needed to run the process and give specific advice.
- Build backups to support infrastructure, such as:
  - computing facilities (for example third-party hot-site backup and mutual arrangements with other institutions), and
  - power (for example emergency generators, UPS systems, and dual-power feeds).
- Develop a Data Backup plan for critical and highly critical data that includes schedules for backups to be sent to a secure off-site storage facility.
- Secure information being transferred to the off-site facility.
- Ensure the data is secure while in off-site storage.
- Develop a Disaster Recovery Plan describing how basic operations (for example, health, office, computing, power, and communications) will run and how data will be restored from backup. Ensure that key staff securely store copies of the plan at home or off site.
- Develop a Business Recovery Plan describing how to restore critical business processes after the Disaster Recovery Plan.
- Include specific recommendations from key personnel. Since you may not have computers available, develop temporary manual procedures. Designate deputies for key staff who may be unavailable.

- In your plans, identify which activities depend on others and the order in which they should be performed.
- Inventory your data (as suggested in the Inventory and Data Classification section) and measure how critical each set is based on the risk analysis. Critical data covers not only personal health information, such as patient records, but also the procedures that protect your institution.

For example:

Not Critical: losing data will be a mere inconvenience with no significant impact

Critical: losing data will cause severe disruption of operations, potential losses and legal liability

Mildly Critical: losing data will inconvenience the institution, but will not cause significant loss or risk liability

Highly critical: losing data will mean institutional failure, risk of injury or loss of life, or criminal liability

- Test your plans once or twice a year to make sure they still work and that backup data is useable.
- The parts of your plans that cannot be tested in practice should be "paper" tested, with all staff involved walking through the plan together to identify potential problems.

Small Office Applicability

- Regularly back up critical personal health information on your computers to removable media (for example CD) at least monthly.
- Store these back-up copies in a secure off-site location. Secure the copies in transfer.

- Periodically test back-up copies before storing them to ensure they are useable. You do not want to find useless copies when you need the back-up.

Development and Maintenance

What You Need To Do

Institute policies to ensure security is considered when developing, buying and maintaining IT resources.

- Spell out the security requirements that IT systems and software should meet to support your security policy. Specify the audit information that you need to check that specified requirements are met.
- We recommend that you follow the HL7 (Health Level 7) standard for application interconnection in any application managing health records (see the Security Standards section).
- Perform a Threat Risk Assessment (TRA) and a Privacy Impact Assessment (PIA) for any major change to systems or software to identify and address any security and privacy concerns (see Appendix B for a sample TRA form). Include appropriate security questions in your normal application development and IT purchasing processes.
- Ensure that all built-in hardware and software security features in the IT products you buy are used properly (including changing administrator passwords from their default values).
- Separate any development, test and production environments. Strictly control the transfer of code between these environments with a rigorous change control process to avoid introducing new security risks.
- Do not use personal health information from your system to test changes in your test and development systems. Strip identifying details from information used outside your environment.
- Regularly monitor software updates and implement code updates designed to address security vulnerabilities.

Small Office Applicability

- Buy software from only reputable vendors. Professional journals and organizations like the Ontario Medical Association may suggest software for practices like yours.
- Promptly install any updates vendors offer to close security vulnerabilities.

Audit

What You Need To Do

Regularly audit your actual practices for compliance with your security policy.

We interpret audit broadly in this section to mean any review of current practices against policy or standards. This includes spot checks to make sure staff with access to personal health information are protecting it appropriately.

- If you have never audited security, conduct a "gap analysis" review.
  - A "gap analysis" review compares a target of acceptable security practices with current practices, revealing a list of gaps between the two.
  - The list of gaps identifies issues needing immediate attention and constitutes a baseline for future audits.
- The Diagnostic Tool in this Toolkit can be used for a preliminary assessment of security gaps. However, we suggest hiring outside experts to conduct the initial audit if your staff lacks the skills. You can always require the experts to train staff if you wish to perform future audits yourself. Do periodic external audits to make sure you keep pace with technology, standards and what similar institutions are doing.
- Conduct security audits at least annually. If internal staff will conduct the audit, choose individuals:
  - without day-to-day responsibility for the practices, and

  - with appropriate skills and current knowledge of security issues, practices and threats.

- A Security Audit should focus on how well actual security practices compare with the institution's security policy, standards and procedures.
- Use random spot checks to help ensure security policies are being followed and determine whether users are following Acceptable Use Policies, such as locking up sensitive information and locking computers.
- Audit the performance of any third parties handling personal health information on your behalf to make sure they meet the security requirements your agreement specifies.
- Perform Threat Risk Assessments (TRA) and Privacy Impact Assessments (PIA) whenever you make major changes to systems or software to make sure you have addressed any security and privacy concerns (a sample TRA form is included with this Toolkit). Follow up and resolve any problems.
- Your audit results and action plans to correct security risks should be:
  - regularly reviewed within the institution's management system (for example monthly senior management operations review), and
  - built into individual managers' performance measures and evaluation systems.
- Make sure you consider problems that will take time to resolve within the institution's risk management process and get the appropriate senior manager to sign off on the risks.
- Design your systems to give you all the information you will need for audits. (Appendix C contains suggestions.)
- Perform both external and internal security penetration tests (sometimes called ethical hacking) at least annually. (You may need to hire outside professionals to provide the necessary expertise and objectivity for the tests).
- Evaluate your security audit program's effectiveness by reviewing:
  - actual security incidents and determining whether your audit program should have caught them, and
  - staffing levels compared with those at similar institutions having effective security programs to ensure your resources are in line.

Appendix C – "Audit" provides more detailed guidance on capturing and using audit information.

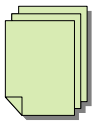
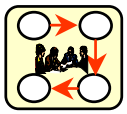
Small Office Applicability

- Perform spot checks on a regular basis to ensure all staff are following the security rules and take appropriate action.

Recommended Standards

What You Need To Know

The emerging international cross-industry standard for security is ISO/IEC 17799. Details of the standard can be found at www.iso.org. The 10 core areas of the framework are summarized below. The topics covered in the above security sections fit into this framework.

Policy	Organization	Asset Classification and Control	Personnel Security	Physical Security
				
Security rules the organization follows	Management framework supporting the policy and ensuring compliance	System to inventory and classify assets so they may be more effectively managed and protected	Rules to reduce the risk of individuals compromising security	Measures to prevent unauthorized access and damage to systems

Sustaining Security

Computer and Network Management	System Access Control	System Development and Maintenance	Business Continuity	Compliance
				
Disciplines to manage IT resources to support security objectives	Mechanisms to ensure that only authorized personnel have access and for only authorized purposes	Disciplines to ensure the IT environment sustains the required security levels	Plan to ensure that critical business activities can be performed if technology fails or local disasters happen	Program to ensure that security measures meet policy and legal and contractual security requirements

Other recommended standards and guidelines include:

- **ITIL (IT Infrastructure Library).** This widely accepted approach to IT Service Management provides comprehensive guidance on best practices for the processes required to support IT, including those critical to security such as Change Management. More details can be found at http://www.ogc.gov.uk/index.asp?id=2261

- **COBIT (Control Objectives for Information Technology).** This widely accepted standard for good Information Technology (IT) security and control practices provides a reference framework for management, users, and IS audit, control and security practitioners. More details can be found at http://www.isaca.org/

- **COACH (Canada's Health Informatics Association).** The COACH-published "Guidelines for the Protection of Health Information," which supplements this Toolkit, provides more detail on how to implement security in a healthcare setting. More details can be found at http://www.coachorg.com/

- **RCMP Guidelines for Threat Risk Analysis (TRA).** Details on this tool for identifying and mitigating security risks can be found at http://www.rcmp-grc.gc.ca (Also see Appendix B for a sample TRA form.)

- **HL7 (Health Level 7).** We recommend any applications managing health records meet the HL7 (Health Level 7) standard for application interconnection. Based on the ISO OSI (Open Systems Interconnection) Level 7 application interconnection standard, this standard is gaining wide acceptance and includes security checks. More details can be found at http://www.hl7.org.

Related Sections of the Act

2, 3, 4, 10, 12, 13, 14, 42, 53

Checklists, Templates and Tools

Appendix A – "Business Continuity" provides a sample Business Recovery and Disaster Recovery Management Guide

Appendix B – "Development and Maintenance" provides more detailed guidance on Secure Applications and a sample TRA form

Appendix C – "Audit" provides more detailed guidance on capturing and using audit information

APPENDIX A – BUSINESS CONTINUITY

Business Recovery and Disaster Recovery Management Guide

1. Establish a Business Recovery and Disaster Recovery Management Process. A Business Recovery and Disaster Recovery management process must be implemented across the organization to reduce an interruption's effects to a level acceptable by service unit management and regulatory authorities.

- Assign a staff member responsibility for Business Recovery planning (Business) for the institution. Also appoint individuals within each service unit performing critical functions and sub-functions.
- Assign a staff member responsibility for Disaster Recovery planning (IT).
- Identify service units critical to the organization, based on criteria management agrees to.
- Define a Business Recovery group with members from each service unit to ensure that adequate recovery plans are instituted and kept current as the business changes.
- Make the Business Recovery group responsible for ensuring that staff from each service unit are assigned and trained on Business Recovery and Disaster Recovery processes and procedures.
- Involve assigned staff in testing the recovery plan (at least annually)
- Review the institution's insurance coverage annually for opportunities to use coverage as an alternative way to manage the risk of an interruption or the organization's response to an interruption

2. Perform a Business Recovery and Disaster Recovery Impact Analysis. Business Recovery and Disaster Recovery planning must be based on the results of a Recovery Requirements Analysis that assesses the impacts of interruptions to critical service. Determine the resources on which those critical functions rely and the maximum period of interruption each critical function can withstand.

- All service units must participate in the Recovery Requirements Analysis.
- The threshold for a critical service unit is based on an analysis of the impact of interruptions to its services and the maximum time those services can withstand interruption.

- Develop strategies to determine the overall approach to Business Recovery and Disaster Recovery and have management endorse them.
- Establish a budget for contingency planning.

3. Develop and Maintain the Business Recovery and Disaster Recovery Plans. Business Recovery and Disaster Recovery Plans will be documented for each service unit identified in the Recovery Requirements Analysis. The plans should:

- include the requirements for alternate sites, hardware, software and service unit specific items,
- make saving human life top priority,
- be supported by documented Crisis Management and Emergency Response procedures and responsibilities,
- include detailed procedures on the tasks the management team must perform when declaring a disaster,
- include detailed procedures on what each service unit must do when a disaster is declared,
- specify authority for activating recovery strategies, such as an alternative location (hot-site) and assign authorities for other specific functions,
- identify the budget that will be made available when declaring a disaster and how the expenditures will be managed during the interruption,
- identify how staff will be informed of the disaster and given instructions on what they should do,
- include the types and frequency of testing required, and
- include maintenance to ensure that currency with business processes and priorities and resource changes.

4. Test the plans. Regularly test Business Recovery and Disaster Recovery Plans to ensure they are up to date and effective.

- Test the plans at least annually or when major changes occur in the organization, priorities or infrastructure
- Testing should range from the following:
    - Table-top dry runs.

  - Simulation testing.
  - Parallel system running.
  - Partial cut-over testing.
  - Full contingency testing.

- Testing may be either planned or unplanned.
- Testing should occur with different staff to ensure cross-training.

5. Maintain and re-assess the plans. Business Recovery and Disaster Recovery plans must be kept current with the business. Use a change management and control process to make sure the plans reflect the organization's current needs. The following changes could affect the plans:

- People with responsibility within specific plans changing functions within the organization
- New business strategies
- New location, facilities or resources
- Amendments to applicable legislation
- New key vendors, personnel, supplies, management or customers
- New service unit processes or priorities
- A service unit providing different services (which could alter whether the unit is designated as a critical service unit).

APPENDIX B – DEVELOPMENT AND MAINTENANCE

General Guiding Principles for Secure Applications

These principles are written for application designers but can also be used to evaluate an application that is being purchased.

- **Avoid Security Through Obscurity.** Assume hackers will inspect source code and design applications accordingly. Secrets, such as hidden fields and path names, may slow an attacker down, but secrets do not stay secret forever. Application security based on "security by obscurity" is doomed to fail.

- **Principle of Least Privilege.** Do not require the application to run on the administrator account. Use coding discipline to determine what privileges actually needed and explicitly grant only the privileges to the non-administrator account on which the application runs.

- **Principle of Least Trust.** Do not trust input external users provide. Assume that external systems are insecure. Vet data and inspect every return code from every function call, including system library routines.

- **Separate Services.** Dedicate a single service to a single platform. Though it may cost less to run multiple services on the same platform, doing so increases the system's overall complexity and increases security vulnerabilities.

- **Principle of Simplicity.** Ensure that security subsystems are manageable and not overly complicated for users and administrators. Large interfaces and complex solutions run a higher risk security vulnerabilities than small interfaces and simple code. The more entrance points available to an application and the more intricate the application's functionality, the higher the potential for bugs, some of which will be security-related. Security functionality added to an application must be easy to install, configure, and use. Otherwise, it will be disabled or bypassed.

- **Avoid a Single Point of Failure.** Applications should never be designed so that a single mechanism failure (such as a firewall or authentication service Failure) jeopardizes the entire application. Also called Defence in Depth, this principle recommends a design where a second mechanism that must be defeated before one mechanism's failure can compromise the application, a third must be defeated if a second fails, and so on. A Buffer Zone is an example of more than single-point failure. If the outer firewall fails, though the web server may be vulnerable and compromised, the rest of the application and data remains safe behind a second firewall.

- **Secure Defaults.** Do not enable services by default unless absolutely necessary. Services should be disabled by default and enabled only by an explicit decision. The default settings should be the secure mode of operation. Security should not have to be turned on; it should always be present unless explicitly disabled.

- **Fail in a secure mode.** Ensure that applications, systems, and subsystems fail in a secure manner. This is called failing closed (as opposed to failing open). Write code to explicitly verify what is allowed before allowing it. Do not attempt to check for the cases where things are disallowed; an event may be missed and the application could fail in a non-secure mode because the failure was not recognized.

  - Examples that translate this principles into design features include:

  - Systems and applications should not store passwords in unencrypted form.

  - Systems and applications should centrally manage time-outs of inactive sessions used to access health information.

  - Applications should have input controls to ensure valid data and prevent data input from causing error conditions.

  - Applications should avoid writing personal information to client devices.

  - Applications should be able to capture and honour any patient consents such as lock-box provisions.

  - Applications should minimize the possibilities for unauthorized transmission, print or cut-and-paste copying.

Sample Threat Risk Assessment Form

Use this sample Threat Risk Assessment (TRA) Form based on RCMP/CSE Methodology. Although a row of sample data is provided, refer to the RCMP website for more guidance. If you have never performed a TRA, consider using outside professional help for your first one.

1. Asset Characteristics							
		Statement of Sensitivity				Effect if Compromised	
#	Description	Value	Confidentiality	Integrity	Availability	Privacy Impact	Potential Loss
1	EHR Database Server	$35K	High	High	High	High	Service, financial, legal, trust
2							
3							

2. Threat Assessment						
#	Threat Details		Exposure			
	Nature	Class	Likelihood	Loss	Impact	Exposure Rating
1	*Server Failure *Computer Component Failure *Criminal Activity *Hacker Activity *Staff Termination *Tampering *IT Malfunctions *Penetration *Theft of Equipment *Theft of Data *Modification of Data *Cryptographic Failure	Disclosure Interruption Modification Destruction Removal / Loss	Medium	Confidentiality Integrity Availability Privacy	High	High
2						
3						

3. Risk Assessment (Current State)				
#	**Safeguard**	**Effectiveness**	**Vulnerability**	**Risk Level**
1	*Identification *Authentication *Authorization *Training *Structural access protection *Climate control *Fire detection/sprinklers *Encryption *Auditing *Testing procedures *Change control procedures *Virus scan *Emergency and contingency planning *A secure physical environment *Limitation of physical access to the server *Strong database management skills *Data reconstruction procedures *Personnel security screening	Medium	Medium	Medium
2				
3				

4. Residual Risk				
#	Mitigation		Outcome	
	Recommendations	Mitigated Risk Level	Decision	Implemented
1	*Applications that draw on information stored within a database, will use the authentication and access controls for authorization provided by the security framework. *Ensure that a Threats and Risks Assessment has been approved for each associated application. *The Database Server should be protected by a firewall for security	Low	Accepted	Yes
2				
3				

APPENDIX C – AUDIT

Guidance on Capturing and Using Audit Information

- Design your processes and systems to capture information from the sources you will need to audit against, such as:
  - application logs (for applications that process personal health information),
  - system logs,
  - network logs,
  - exception logs (for example, failed logon attempts),
  - operator logs,
  - badge access or sign-in logs for restricted areas, and
  - sign-out logs for hardcopy personal health information.
- Make sure these logs contain the information required for your audit analysis and keep them secure.
  - Collect identifying information, such as User ID, the time and date, terminal location, resource being accessed, application being used, and the action being taken on personal health information (for example, view, update or delete).
  - Collect event information, such as failed access attempts, intrusion alerts and other management alarms, policy violations (for example, firewalls) and system failures.
  - Do not store logs on the same server being monitored.
  - Protect logs against destruction or unauthorized changes (users with privileged support IDs should not be able to alter or erase logs).
- Determine a strategy for using the audit information you collect:
  - Start with exceptional incidents where the record captures potentially threatening events, such as excessive failed access attempts.

- Adopt a spot-checking approach, such as reviewing the activity of a user ID (especially privileged IDs) over a period of time to check for regularity. review access to particular records to ensure appropriateness. Access to some records may be worth watching more closely than others (for example those of a well-know politician, celebrity or senior manager).

- If the spot-checks reveal many potential problems or miss problems discovered through other means, increase the frequency.

- Whenever possible, use automated tools to scan the logs and find correlations that may indicate possible intrusion attempts, unauthorized or illegal activities, or suspicious events, such as activity beyond normal bounds of a job role, that require further investigation.

Research

Table of Contents

Key Points

- The Act sets out specific requirements for the collection, use and disclosure of personal health information for research that is conducted without consent.
- The research provisions of the Act apply to:
  - *researchers*, who *collect* and *use* personal health information for research purposes,
  - *health information custodians* (such as hospitals and physicians), who *disclose* personal health information for research purposes, and
  - *research ethics boards*, who review and approve research plans.
- This Toolkit uses the term "you" for the sake of brevity. In this section, the term "you" refers to the health information custodians and researchers reading this section, who must observe the Act's requirements concerning research in their respective roles.
- You may *collect* personal health information for research purposes without consent from non-health information custodians who are not prohibited by law from disclosing the information to you, and from health information custodians who are permitted or required by law to disclose the information to you. Before collecting the information without consent, you must comply with the Act's requirements concerning research plans and research ethics board approval.
- You may *use* personal health information for research purposes without consent if a law permits you to do so. To use personal health information for research purposes without consent, you must comply with the Act's requirements concerning research plans and research ethics board approval. When conducting research under the approved research plan, you must follow the research duties that are listed in the Act.
- You may *disclose* personal health information to a researcher without consent; however, before disclosing the information to a researcher, you must enter into a written agreement with the researcher to protect the information, and receive from the researcher a written application, a written research plan and a copy of the research ethics board's approval of the research plan from the researcher. You may also impose any other obligations on the researcher that you feel are appropriate.

Research

The Rule

You may collect, use and disclose personal health information for research purposes without consent, but only if you meet the strict conditions described below.

- The research provisions of the Act apply to:
  - *researchers*, who *collect* and *use* personal health information for research purposes,
  - *health information custodians* (such as hospitals and physicians), who *disclose* personal health information for research purposes, and
  - *research ethics boards*, who review and approve research plans.
- This Toolkit uses the term "you" for the sake of brevity. In this section, the term "you" refers to the health information custodians and researchers reading this section, who must observe the Act's requirements concerning research in their respective roles.
- The Act has rules on dealing with personal health information, but does not have specific rules on dealing with specimens. You should follow standard best practices when dealing with specimens in research, in addition to the rules in the Act.
- This section of the Toolkit deals with retrospective research for which consent is not obtained. It does not discuss clinical trials, genetic testing or other studies, for which express consent is required.
- This Toolkit only deals with privacy issues. A discussion on other ethical issues relating to research, including risks and harms, is beyond the scope of this Toolkit.
- Nothing in the Act prevents you from collecting, using or disclosing personal health information for research purposes with *express consent*. You may not rely on *implied consent* to collect, use or disclose personal health information for research purposes.

What You Need To Do

Collection

You may collect personal health information for research purposes indirectly and without consent:

- from non-health information custodians (such as family members) who are not prohibited by law from disclosing the information to you,
- from health information custodians who are permitted by law to disclose the information to you, and
- if you are permitted or required by law to collect the information indirectly and without consent.

However, before doing so, you must comply with the Act's requirements concerning research plans and research ethics board approval (which are described below).

The person disclosing the information will ask you to enter into a written agreement concerning protection of the information (which might address the information's use, security, disclosure, return or disposal).

Note: If someone within your hospital provides the information to you, you will likely be asked to sign a Confidentiality Agreement. If someone external to the hospital discloses the information to you, you will likely be asked to sign an Information Sharing Agreement.

Use

You may use personal health information for research purposes without consent if a law permits you to do so.

However, when doing so, you must:

- conduct your research under a research plan that a research ethics board has approved (as described below), or
- follow the rules for research approved outside Ontario (as described below) if the personal health information originates outside Ontario.

When using personal health information for research purposes without consent, you must submit a research plan to a research ethics board outlining your anticipated use of the information.

Once a research ethics board approves your plan (or, in the case of information originating outside of Ontario, a similar research approval body), you must follow the Researcher Duties described below.

If you do not have a research ethics board at your facility, you must have some other research ethics board approve your research plan.

Disclosure

You may disclose personal health information to a researcher without consent if you enter into a written agreement with the researcher to protect the information (which may address its use, security, disclosure, return or disposal) (for disclosure outside the hospital), and receive from the researcher:

- a written application,
- a written research plan (meeting the requirements described below), and
- a copy of a research ethics board's approval of the research plan.

The discretion to grant requests for disclosure remains with you and you may impose additional obligations on the researcher.

Research Plan

The research plan must describe all of the matters listed on the Research Approval Checklist.

Research Ethics Board Composition

A research ethics board must be composed of at least five members, including:

an independent member

a member knowledgeable in research ethics

two members with relevant expertise in the research

a member knowledgeable in considering privacy issues

Research Ethics Board Duties

A research ethics board reviews research plans prepared by researchers. Members of a research ethics board must not review proposals with which they have a conflict of interest.

If the research ethics board is deciding whether to approve a research plan for research to be conducted without consent, it must consider everything relevant, including:

- whether the researcher could reasonably achieve the research goals without using personal health information,
- whether the researcher will put adequate safeguards in place to protect privacy and preserve the information's confidentiality,
- the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose information is being disclosed, and
- whether it would be impractical to require the researcher to get the affected individuals' consent.

A research ethics board should ensure that it considers all matters listed on the Research Approval Checklist. Once it makes a decision, a research ethics board must explain to the researcher in writing:

- whether the research plan has been approved,
- why it has been approved or denied, and
- if approved, whether the approval is subject to any conditions.

Researcher Duties

As a researcher, you must:

- comply with the approved research plan, including any conditions imposed by the research ethics board,
- implement the safeguards for protecting the information (see security and storage guidelines) outlined in your plan,
- use personal health information only for the purposes described in your research plan,
- not publish personal health information in a way that could reasonably allow others to identify the individual whose information was used in the research,
- only disclose the information when required by law,
- not contact individuals whose information is used in the research unless they have given consent to the disclosing health information custodian to be contacted by you (even if personal health information you hold is stolen, lost or accessed by unauthorized individuals),

  Note: The health information custodian who collects the information would obtain this consent.

- comply with the terms and conditions of the written agreement that you enter into with the disclosing health information custodians, and

  Note: Hospitals should develop a clear policy on signing these agreements, which includes the designation of a person responsible for them.

- provide written notice of any breach of the written agreement or any of these duties to the disclosing health information custodians.

If you work under a research plan approved outside Ontario, you must follow the same requirements that researchers whose plans are approved in Ontario must follow.

You may use or disclose personal health information originating outside Ontario for research purposes without consent if a research ethics board (or other body outside Ontario responsible for approving research) has approved the research.

Disclosure Under Other Acts

You must still follow all of the above disclosure rules, where another law allows you to disclose personal health information to a researcher without consent (for example, to Cancer Care Ontario as a researcher).

Transition Rules

The Act provides a three-year transition period for all research projects approved before November 1, 2004.

This means that if you have been using or disclosing personal health information for research purposes without consent within the three years before November 1, 2004 and your research will not continue past November 1, 2007, you do not need to take any additional steps.

If your research will continue past November 1, 2007, however, you must take steps to comply with the Act.

Express Consent

Nothing in the Act prevents you from collecting, using or disclosing personal health information for research purposes with *express consent*. You may not rely on *implied consent* to collect, use or disclose personal health information for research purposes.

The strict conditions described above apply to research that is conducted without consent. As a best practice, you should still comply with these conditions when you collect, use and disclose personal health information for research purposes with express consent.

The research rules in the Act relate to retrospective research for which consent is not obtained. You must obtain express consent when you conduct clinical trials, genetic testing or other research that is not simply retrospective.

For additional guidelines on researching with express consent, see the Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans.

Related Sections of the Act

Sections 2, 3, 4, 12(3), 36(1)(a), 36(1)(d), 36(1)(g), 36(1)(h), 37(1)(a), 37(1)(b), 37(1)(j), 36(1)(k), 37(3), 44 of the Act

Sections 11, 15, 16, 17 and 18 of the General Regulation

Checklist, Templates and Tools

- Research Approval Checklist
- Sample Research Application
- Sample Information Sharing Agreement
- Sample Consent Form

RESEARCH APPROVAL CHECKLIST

The research plan must describe:

- ❑ the name, affiliation, roles and qualifications of everyone working on the research and accessing personal health information
- ❑ adequate justification for disclosing personal health information to these persons
- ❑ the nature of the research
- ❑ the particular research objectives and related research questions
- ❑ the duration of the research
- ❑ the anticipated public and scientific benefit of the research
- ❑ the required personal health information
- ❑ the sources of the personal health information
- ❑ the use of personal health information, including details on information linkage (if any)
- ❑ adequate justification for using the personal health information
- ❑ adequate justification for linking the personal health information
- ❑ adequate consent process/form OR adequate justification for proceeding without consent
- ❑ the reasonably foreseeable harms and benefits of the information use
- ❑ adequate explanation of how foreseeable harms will be addressed
- ❑ adequate privacy and security safeguards
- ❑ how long the information will remain identifiable and why
- ❑ how and when the information will be destroyed or returned to source
- ❑ details on research funding
- ❑ details on whether the researcher has applied for other research ethics board approval and its response or the status of the application
- ❑ details on the researcher's conflicts of interest
- ❑ details on any additional matters the law or ethical guidelines and conventions may require

REB File No.:
Date:

SAMPLE APPLICATION TO RESEARCH ETHICS BOARD

A. GENERAL INFORMATION

PRIMARY INVESTIGATOR

Name | Signature

Dept./Div. | Position

Qualifications | Email Address

CO-INVESTIGATOR

Name | Signature

Dept./Div. | Position

Qualification | Email Address

CO-INVESTIGATOR

Name | Signature

Dept./Div. | Position

Qualification | Email Address

OTHER RESEARCH TEAM MEMBERS WHO ARE NOT CO-INVESTIGATORS Please type names, roles and qualifications (signatures not needed)

B. DETAILS OF PROJECT

1. Project Title _____

2. Is this project funded? _____

   ☐ NO

   ☐ YES

3. Sponsor _____

4. Duration of Funding: from __/__/__ to __/__/__

5. Conflict of Interest Declaration – Do you have any conflicts of interest (actual, apparent, perceived or potential) relating to this project?*

   ☐ NO

   ☐ YES

   Description of conflict of interest _____

   Mandatory Signature _____

   (Application will be returned without signature)

   *Conflicts of interest include but are not limited to the following situations and also must be disclosed under institutional policy for review: If you or any of the involved research team members or your/their dependants have:

   (1) employment or consulting arrangements and/or a financial interest in the sponsor of the study, or with proposed subcontractors, vendors or collaborators; or

   (2) a financial interest in the subject of the study.

6. Protocol:

   a) *Nature*

   b) *Objectives*

   c) *Methods*

d) *Statistical Analysis*

e) *Anticipated Public or Scientific Benefit*

f) *Duration of Research*

g) *Foreseeable Harms and Benefits of Research (describe how harms will be addressed)*

C. INFORMATION REQUESTED

1. What patient information do you require?

_____

_____

2. What patient information source are you accessing?

☐ Health Records Clinic/Office Files	Specify which
☐ Electronic Database	Specify which
☐ Outside Institution	Specify which
☐ Other	Specify which

3. Proposed number of research subjects _____

4. Are you requesting information that identifies or potentially identifies individuals?

☐ NO
☐ YES

If yes, explain why you cannot use anonymized or aggregate information:

_____

_____

5. Have you obtained consent from the individuals to collect and use the identifying information on this project?

☐ YES Attach a sample consent form

☐ NO

If no, explain why

_____

_____

6. What security measures will be in place to protect the information during transmission?

_____

_____

D. INFORMATION LINKAGE

1. Does your project involve linking any information from this request to other information?

☐ NO
☐ YES

If yes,

Describe what information is to be linked:

_____

_____

Describe what type of linkage is required:

_____

_____

Describe the rationale for this linkage:

_____

_____

2. Have you received approval from the other information sources including division/department head authorization to conduct this linkage?

☐ NO

☐ YES Please attach the approval(s)

3. Will the information be retained in linked form?

☐ NO

☐ YES

4. When will the information be de-identified after the linkage?

_____

_____

E. DISSEMINATION OF ANALYSIS AND/OR REPORTS:

1. How do you plan to disseminate and/or publish the results of your analyses?

_____

_____

2. What is the expected date of dissemination and/or publication?

_____

F. DISCLOSURE AVOIDANCE PRACTICES

1. How will you ensure that information will be aggregated prior to disclosure, to the level required in the information sharing agreement, confidentiality agreement, privacy policy and other applicable policies and procedures?

_____

_____

_____

2. Attach information collection form or list of fields (mandatory: application will be returned if this information has not been included)
Please note that the content of the form should be adequate to answer the research questions.

3. Are any sensitive issues raised in this study or its publication (e.g. HIV status, mental health status, subjects identifiable, pedigrees, other)

☐ NO

☐ YES Please specify _____

G. SECURITY AND ACCESS

1. The information obtained from the records described above will be used for the outlined research purposes only:

☐ NO If no, a separate request must be submitted
☐ YES

2. List all of the persons who will have access to the records in an individually recognized form for the research purpose described and why they need this access: (name and role in research)

_____

_____

3. Have all these persons signed confidentiality agreements?

☐ NO

☐ YES If no, please indicate when agreement will be signed

_____

_____

H. SECURITY MEASURES

1. Describe how you will keep information secure

☐ Premises will be locked except when one or more of the individuals named in E1(b) are present

☐ Access to the premises will be controlled (passcards, security clearances etc.)

☐ Access to the information will be restricted to the research team by:

☐ Patient code ☐ Files/Folders password ☐ Computer password

Please provide name of password software_____

☐ Other computer security methods that prevent unauthorized access will be used

☐ Encryption ☐ Firewalls ☐ Identifying Information Scrambled/De-linked

Other (Describe):_____

☐ Staff will be trained regarding privacy

☐ Staff will sign a confidentiality agreement

☐ Other, explain

_____

_____

2. Will information remain within the institution?

☐ NO

☐ YES If no, please indicate why and how information will be exported outside

_____

_____

3. Will system files be backed up automatically?

☐ NO
☐ YES

If yes, please specify provisions that would be made for a private drive that cannot be accessed by anyone other than your research team, or that could not be backed up by computer support staff within your organization:

_____

_____

All original personal health records received from ● must be returned to ● and all copies of personal health records that were made or received must be destroyed in accordance with the information sharing agreement.

I certify that the information reported here is accurate and that the personal health information will not be used for future projects without prior approval of a research ethics board.

Primary Investigator Signature _____ Date _____

Division/Department Head Signature of Approval _____ Date _____

Do you plan on accessing information from another division/department?

☐ NO
☐ YES If yes, authorization from the division/department head is requested

Signature of Approval _____ Date _____

In making this request, I acknowledge that failure to comply with the terms and conditions of the information sharing agreement is cause for termination of the agreement and, where applicable, a complaint to the Information and Privacy Commissioner/Ontario.

Date _____ Signature of Requestor _____

Research Ethics Board for Retrospective Research

Signature of REB Chair _____

Date of Approval _____ Approval Expires _____

Level of Continuing Review:

NOTE TO USER: This Sample Information Sharing Agreement is intended to be used for retrospective research. You should consider using a material transfer agreement if your research involves the transfer of specimens. A customized version of this Sample Information Sharing Agreement could be used when a hospital discloses personal health information to a health data institute for research purposes. It would not typically be used when a health information custodian shares personal health information with a researcher from the same hospital; however your confidentiality agreement with your internal researcher should include many of the same standards for confidentiality contained here. Hospitals should develop a clear policy on drafting, negotiating and signing these agreements, which includes the designation of a person responsible for them.

SAMPLE INFORMATION SHARING AGREEMENT

This Information Sharing Agreement is effective as of **[insert date]** between **[insert name of Hospital]** (as the disclosing party) and **[insert name of Researcher]** (as the collecting party)

BACKGROUND:

A. **[Identify the Hospital.]**

B. **[Identify the Researcher.]**

C. **[Outline the details of the proposed disclosure of personal health information and the research.]**

D. The parties now wish to set out terms and conditions about the collection, transmission, use, retention, disclosure and disposal of certain personal health information provided by the Hospital to the Researcher.

E. Section 44 of the Act gives the Hospital and the Researcher statutory authority to engage in this collection, use and disclosure.

F. **[Identify any other legislative authority for the collection, use and disclosure of the personal health information, such as legislation that governs the parties or the research.]**

FOR VALUE RECEIVED, the parties agree as follows:

SECTION 1 - INTERPRETATION

1.1 Definitions

In this Agreement:

(1) ***Act*** means the *Personal Health Information Protection Act, 2004* (Ontario) and where the context requires includes the regulations under that Act, including any amendments;

(2) ***Hospital*** means **[insert name of Hospital]**;

(3) ***Research*** has the meaning set out in Section 2.2(1);

(4) ***Research Plan*** means the research plan attached as Schedule A;

(5) ***Researcher*** means **[insert name of Researcher]**;

(6) ***Shared Information*** has the meaning set out in Section 2.1;

(7) **[Include definitions of any terms or acronyms that may be unique to the subject matter of the Agreement.]**

1.2 Purpose of Agreement

The purpose of this Agreement is to set out terms and conditions about the collection, transmission, use, retention, disclosure and disposal of the Shared Information that is provided by the Hospital to the Researcher for the purposes described in Section 2.2(1) and Schedule A.

SECTION 2 - INFORMATION SHARING

2.1 Shared Information

The Hospital will provide to the Researcher the personal health information described in Schedule B (the "Shared Information").

2.2 Use of Personal Health Information

(1) The Researcher shall use the Shared Information, and shall ensure that the Shared Information is used, only as necessary to fulfill the specific research objectives and related research questions described in the Research Plan (the "Research").

(2) The Researcher shall not collect or use the Shared Information for any purposes other than those purposes described in Section 2.2(1) and Schedule A or specifically authorized by legislation.

(3) The Researcher shall require the prior approval of the Hospital for any proposed changes to the Research described in Section 2.2(1) and Schedule A.

(4) The Researcher confirms that the Research Plan has been approved by the **[insert name of research ethics board]** on **[insert date]** and that a copy of the **[insert name of research ethics board]**'s written approval of the Research Plan is attached as Schedule C.

(5) The Researcher agrees that the Researcher shall comply with the conditions imposed by the **[insert name of research ethics board]** concerning the Research Plan, if any.

2.3 Method of Sharing Information

(1) The Hospital will provide to the Researcher the Shared Information via **[specify manner of information sharing such as provision of a computer tape, computer disk, hard copy, electronic data interchange, etc.)]**.

(2) Such transmission of Shared Information will take place on **[specify frequency of sharing]**.

(3) Such transmission of Shared Information will **[describe the measures that will be taken to ensure that the Shared Information will be protected against loss and unauthorized access during transfer]**.

2.4 Accuracy, Completeness and Currency of Shared Information

The Hospital may conduct audits in accordance with an information quality framework and may follow up with the Researcher concerning the maintenance of appropriate technical standards for information quality, integrity and security in order to seek to ensure the accuracy, completeness and currency of the Shared Information. The Researcher shall fully cooperate with the Hospital in this regard. **[If this provision is not appropriate in the circumstances, describe what steps will be taken to ensure the accuracy, completeness and currency of the Shared Information before it is disclosed to the Researcher]**.

2.5 Access to the Shared Information

The Researcher shall refer individuals seeking access to their own personal health information that forms part of the Shared Information to the Hospital. The Researcher will cooperate with the Hospital and these individuals in providing access to this information.

2.6 Security of Shared Information

(1) The Researcher shall comply with the Act and all statutes, regulations, rulings and orders relating to the collection, use and disclosure of personal

health information in respect of the Shared Information, as the same may apply or be amended from time to time.

(2) The Researcher shall implement the following security safeguards in handling the Shared Information:

[Insert appropriate provisions. The following provisions are examples of best practices. You should try to include all of these provisions in your agreements; however, it is likely that the Researcher will resist some of these high standards. Consult your lawyers when negotiating these agreements.]

(a) The Researcher shall not disclose the Shared Information, except as permitted by this Agreement or required by law;

(b) The Researcher shall give access to the Shared Information, in a form in which the individual to whom it relates can be identified, only to the Researcher's staff members listed in Schedule D (the "Named Staff"). The Named Staff are responsible for encrypting identifying numbers, linking files, storing and retrieving files from safes that are located in secure rooms and for destroying information in accordance with Section 2.6(2)(m);

(c) Identifying information, including names and numbers, forming part of the Shared Information will be encrypted immediately after the applicable computer program first links the Shared Information;

(d) The Researcher's working files will not contain any identifying information about an individual but will contain the encrypted number;

(e) Other than the Named Staff, staff members of the Researcher will access the working files only in an anonymized form and will produce analyses required for reports from such files;

(f) All of the Researcher's staff members, including the Named Staff, shall sign a confidentiality agreement in a form acceptable to the Hospital;

(g) The Researcher shall take appropriate disciplinary action against any Named Staff member who breaches the terms of his or her Confidentiality Agreement in relation to the Shared Information and shall deny such individual any further access to the Shared Information;

(h) The Researcher shall keep the Shared Information in a physically secure manner at all times **[Consider adding details of physical security.];**

(i) The Researcher shall monitor access to the Shared Information to ensure security;

(j) The Researcher shall allow the Hospital to inspect the Researcher's security arrangements at any time upon reasonable notice and shall notify the Hospital of any material changes to these practices;

(k) The Researcher shall present only aggregated information in its reports so as to prevent any identification of individuals, whether direct or indirect. The Researcher shall ensure that each cell has at least five observations, unless express written authorization for fewer cells is provided by the Hospital;

(l) The Researcher shall not contact any individual to whom the Shared Information relates without the Hospital's prior approval **[The Hospital must ensure that it has the individual's consent to being contacted by the Researcher before giving its approval.]**;

(m) The Researcher shall retain the Shared Information for as long as necessary to fulfill the purposes identified in Section 2.2. The parties will review the Researcher's information retention practices as required;

(n) The Researcher shall destroy, in a secure manner, information that is no longer required to fulfill the purposes identified in Section 2.2. Such information shall be permanently erased, rendered anonymous or destroyed in such a way that it cannot be reconstructed or retrieved. The Researcher shall provide the Hospital with confirmation in writing of the destruction and manner of destruction of the Shared Information; and

(o) The Researcher shall notify the Hospital in writing immediately upon becoming aware that any of the terms or conditions of this Agreement has been breached.

(3) If a Named Staff member no longer has access to the Shared Information in a form in which the individual to whom it relates can be identified, the Researcher shall so notify the Hospital in writing. The Researcher shall be entitled to substitute another individual for that Named Staff member by notice in writing to the Hospital. After the Hospital has been given such

written notice, the substituted individual shall be deemed to be a Named Staff member under this Agreement.

(4) In the event that the Hospital has concerns about the Researcher's compliance with the provisions of this Agreement, the Hospital shall provide the Researcher with written notice of such concerns and its reasons for them. The Researcher shall, within five days of receipt of the notice, investigate the matter and provide the Hospital with a report stating the cause of the deficiency, if any, and the steps taken to prevent a recurrence, if required.

(5) If the Researcher becomes aware that a person has obtained access to the Shared Information other than in accordance with this Agreement through the Researcher's breach of this Agreement, or the Researcher or the Researcher's staff members have used or disclosed the Shared Information other than in accordance with this Agreement, the Researcher shall immediately notify the Hospital in writing and meet any requirements prescribed by law.

(6) The Researcher shall keep the Hospital appraised of any changes to its policies and procedures followed in respect of the Shared Information.

(7) Each party undertakes to give the other written notice of any changes in legislation, regulations or policies governing or regulating it that are likely to affect the parties' rights and obligations under this Agreement.

(8) Upon expiration or termination of this Agreement, the Researcher shall continue to protect the Shared Information in accordance with Section 2.6.

2.7 Term and Termination

(1) This Agreement shall start on **[insert start date]** and shall end on **[termination date]**, unless ended earlier in accordance with Section 2.7(2) or if the parties agree in writing to extend it. **[State whether the proposed information sharing will be a one-time occurrence, time-limited, or ongoing.]**

(2) This Agreement may be terminated in any of the following ways:

(a) by written agreement of the parties;

(b) by either party, if written notice of termination is given to the other party, because:

(i) the other party fails to perform or comply with any term or condition of Section 2.6 and such failure to perform or comply is not remedied within **[five]** days of written notice to do so; or

(ii) the other party fails to perform or comply with any material term or condition of this Agreement (other than a term or condition contained in Section 2.6) and such failure to perform or comply is not remedied within **[ten]** days of written notice to do so.

(3) Notwithstanding the termination of this Agreement for any reason, a research project of the type referred to in Section 2.2 may be completed provided that the Researcher has obtained written authorization from the Hospital to do so and the Researcher continues to comply with the terms and conditions contained in this Agreement in respect of that research project.

2.8 Indemnity

In addition to any other protections from liability available to the Hospital at law, the Researcher shall indemnify and hold harmless the Hospital and its directors, officers, employees, agents and medical staff members against any and all third party civil or administrative actions, claims or proceedings, including reasonable legal fees, incurred by the Hospital in connection with any failure by the Researcher or any person for whom it is responsible at law to perform its obligations under this Agreement.

SECTION 3 - GENERAL

3.1 Entire Agreement

This Agreement constitutes the entire agreement between the parties concerning the information sharing described in this Agreement.

3.2 Amendments

This Agreement may be amended only by written agreement of the parties.

3.3 Severability

Each provision contained in this Agreement is distinct and severable. Any declaration by a court of competent jurisdiction of the invalidity or unenforceability of any provision or part of a provision will not affect the validity or enforceability of any other provision of this Agreement.

3.4 Waiver

The failure of either party to insist upon strict performance of any terms and conditions or to exercise any of its rights set out in this Agreement shall not constitute a waiver of these rights, and these rights shall continue in full force and effect.

3.5 Assignment and Enurement

The Researcher may not assign the Researcher's rights or obligations under this Agreement without the prior written consent of the Hospital. This Agreement enures to the benefit of and binds the parties and their respective successors and permitted assigns.

3.6 Survival

Sections 2.5, 2.6 and 2.7(3) shall survive the expiration or termination of this Agreement indefinitely.

3.7 Delivery by Fax and in Counterparts

This Agreement may be executed and delivered by fax and in any number of counterparts, each of which when executed and delivered is deemed an original but all of which when taken together constitute one and the same instrument.

3.8 Governing Law

This Agreement is governed by, and is to be construed and interpreted in accordance with, the laws of the Province of Ontario and the laws of Canada applicable in the Province of Ontario. Each of the parties irrevocably submits to the non-exclusive jurisdiction of the courts of the Province of Ontario.

The parties have executed this Agreement.

[INSERT NAME OF HOSPITAL]

By: _____

Name: ●

Title: ●

[If the Researcher is an individual, use the following signing lines]

SIGNED, SEALED AND DELIVERED in the presence of:

_____
Witness

By: _____
Name: **[Insert name of Researcher]**
Title: ●

[INSERT NAME OF CORPORATION]

By: _____
Name: ●
Title: ●

Schedule A – Research Plan

[Attach the Research Plan, which has been approved by a research ethics board and which describes in detail:

- the name, affiliation, roles and qualifications of everyone working on the research and accessing personal health information,
- adequate justification for disclosing personal health information to these persons,
- the nature of the research,
- the particular research objectives and related research questions,
- the duration of the research,
- the anticipated public and scientific benefit of the research,
- the required personal health information,
- the sources of the personal health information,
- the use of personal health information, including details on information linkage (if any),
- adequate justification for using the personal health information,
- adequate justification for linking the personal health information,
- adequate consent process/form OR adequate justification for proceeding without consent,
- the reasonably foreseeable harms and benefits of the information use,
- adequate explanation of how foreseeable harms will be addressed,
- adequate privacy and security safeguards,
- how long the information will remain identifiable and why.

- how and when the information will be destroyed or returned to source,
- details on research funding,
- details on whether the researcher has applied for other research ethics board approval and its response or the status of the application,
- details on the researcher's conflicts of interest, and
- details on any additional matters the law or ethical guidelines and conventions may require.]

Schedule B – Shared Information

[List all elements of personal health information that will be disclosed to the Researcher for the specified research objectives and related research questions. Only those components of personal health information that are absolutely necessary to achieve the research objectives and to answer the related research questions should be disclosed.]

Schedule C – Research Ethics Board Approval

[Attach a copy of the written decision of the Research Ethics Board. The entire decision, with conditions, if any, must be attached.]

Schedule D – Named Staff

[List appropriate individuals. Limit these individuals to a small number.]

SAMPLE CONSENT FORM FOR STUDY PARTICIPANT

Note to User: This Sample Consent Form is intended to be used for retrospective research. It is not appropriate to use it for clinical trials.

Study Title: ●

Primary Investigator: ●

Sponsor: ●

Background: **[Insert details about the study.]**

What is involved? ●

Benefits and Risks: ●

Voluntary: Participation in this study is completely voluntary. You can refuse to sign this consent form and to participate in the study. You can also withdraw your consent any time by writing to ●. Your care at ● will not be affected by your decision.

Confidentiality: **[Insert details about collection, use, disclosure, storage and disposal of personal health information.]**

You have had this study explained to you and had an opportunity to ask questions. You have been given a copy of this Consent Form. If you have any additional questions about the study, please contact ● at ●. If you have any additional questions about your privacy, please contact ● at ●.

Participant Consent

I agree to participate in this study.

I also permit ● to collect, use and disclose health information about me for the purposes of this study.

Name of Participant (print)	Signature of Participant
Investigator's Signature	Signature of Substitution Decision-Maker (if required)
Date	

Fundraising

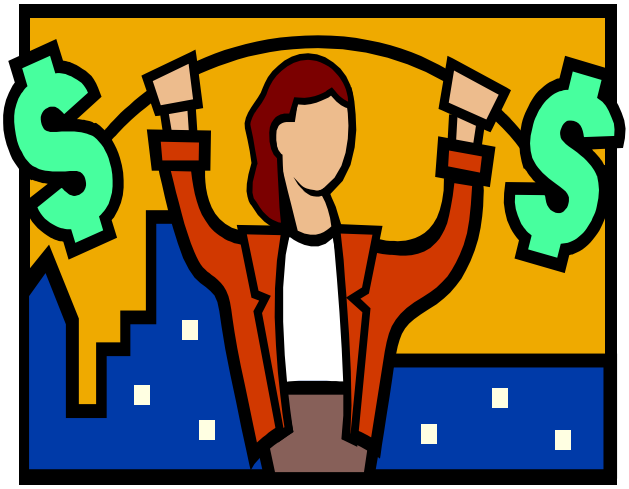


Table of Contents

Fundraising

Key Points

- A hospital may collect, use and disclose information about its patients for fundraising so long as the hospital has its patients' implied consent and the information collected, used or disclosed for fundraising purposes is limited to the patient's name and mailing address.
- You must obtain express consent when you collect, use or disclose more than the patient's name and mailing address for fundraising.
- You must not communicate a patient's state of health or health care when you contact them for fundraising purposes.
- You should require your hospital foundation to follow an appropriate privacy policy.
- You should follow the guidelines on Managing Contracts and Agents if you transfer patient information to others who raise funds for you.
- These fundraising rules also apply to fundraising activities directed at substitute decision-makers, and the collection, use and disclosure of their personal information.

Fundraising

The Rule

A hospital may collect, use and disclose information about its patients for fundraising so long as the hospital has its patients' implied consent and the information collected, used or disclosed for fundraising purposes is limited to the patient's name and mailing address.

You must obtain express consent when you collect, use or disclose more than the patient's name and mailing address for fundraising.

You must not communicate a patient's state of health or health care when you contact them for fundraising purposes.

These fundraising rules also apply to fundraising activities directed at substitute decision-makers, and the collection, use and disclosure of their personal information.

Note: "Patient" refers to an in-patient or out-patient of the hospital facility, service or program.

What You Need To Do

Relying on Implied Consent

You can rely on implied consent when you collect, use and disclose only patient names and mailing addresses for fundraising purposes.

You can rely on implied consent by:

- telling patients that, unless they request otherwise, you will use and disclose their names and mailing addresses for fundraising purposes.

- telling patients how they can easily opt-out of receiving fundraising solicitations in your notices, signs and brochures, as well as in every fundraising solicitation, and
- giving patients 60 days to opt-out of receiving fundraising solicitations before contacting them.

If a patient opts-out within the 60-day period, you do not have their implied consent. If a patient opts-out after the 60-day period, you must treat this as a withdrawal of consent.

See the Consent section for additional guidelines on relying on implied consent.

Obtaining Express Consent

If you obtain express consent, you can collect, use and disclose whatever information the patient has given you permission to collect, use and disclose for fundraising purposes (such as the patient's name, mailing address and place of employment).

However, you should only collect, use and disclose information that is necessary for fundraising. Do not collect more information than you need.

You cannot disclose a list of patients with a common medical condition for fundraising purposes (for example, lung cancer patients for lung cancer research fundraising) without express consent. Such a list contains more than just names and mailing addresses – it also contains specific information about a patient's medical condition. However, specialty hospitals (such as cancer, paediatric and rehabilitation hospitals) do not need express consent to use and disclose patient names and mailing addresses for fundraising purposes.

See the Consent section for guidelines on obtaining express consent.

Disclosing Information to the Hospital Foundation

Hospitals who have obtained consent (express or implied) may disclose information to their own hospital foundation for fundraising.

Hospitals should tell patients (either in person, or through notices, signs or brochures) that this information may be disclosed to the hospital foundation for fundraising purposes as permitted under the Act.

You should require your hospital foundation to follow an appropriate privacy policy.

You should obtain the hospital foundation's commitment that information you have provided will only be used for fundraising.

Providing Information to Hired Fundraisers

If you transfer patient information to others who raise funds for you, you should follow the guidelines on Managing Contracts and Agents.

Related Sections of the Act

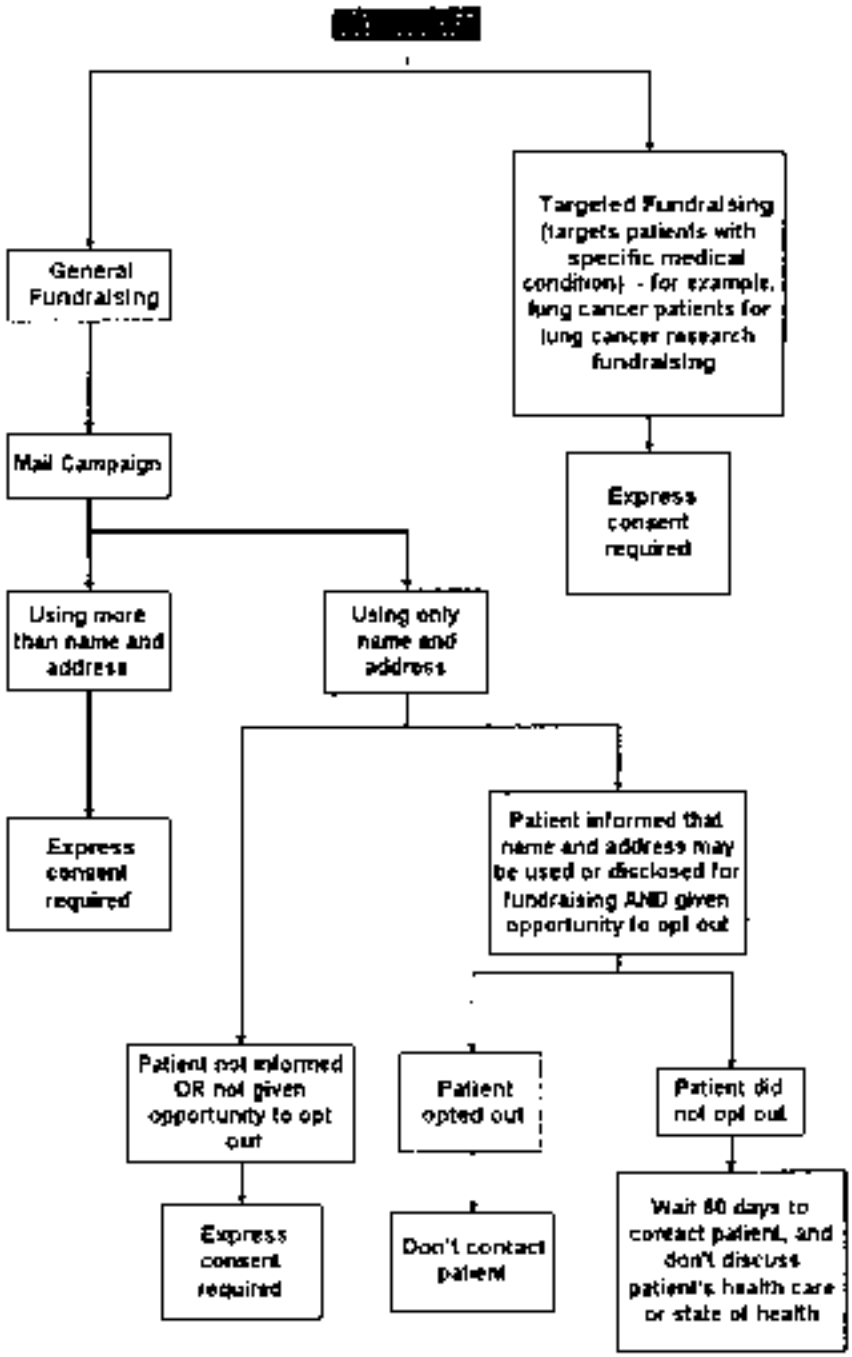
Sections 2, 3, 4, 17, 18(4)(b), 32, 49 of the Act

Section 10 of the General Regulation

Checklists, Templates and Tools

- Fundraising Decision Tree
- Consent Form for Fundraising
- Withdrawal of Consent Form for Fundraising

FUNDRAISING DECISION TREE



Note: "Patient" refers to an in-patient or out-patient of the hospital facility, service or program.

SAMPLE CONSENT FORM FOR FUNDRAISING

Consent to the Collection, Use and Disclosure of Personal Information for Fundraising Purposes

We may use personal **[demographic]** information about you, including your name and mailing address, in order to contact you to support our fundraising programs. We may also share this information with **[our hospital foundation]**, which will contact you on our behalf. By signing below, you permit us to contact you with information on our fundraising campaigns at a later date.

You can refuse to sign this consent form. You can also withdraw your consent any time by writing to ●. Your refusal or withdrawal of consent will in no way affect the care or treatment that you receive at **[Hospital]**.

Patient Consent

I, _____ authorize **[Hospital]** to collect, use and disclose:
(First and Last Name)

☐ just my name and mailing address
☐ my name, mailing address and the following personal information.

_____

[Note to User: Consider inserting the personal information you would like to use for fundraising purposes, such as email address, telephone number, etc.]

for use in fundraising relating to the **[Hospital]**'s charitable activities. I understand that you might share information about me with the hospital foundation.

Name: _____

Address: _____

_____

Signature: _____ Date: _____

FOR INTERNAL OFFICE USE ONLY

Patient ID No: _____

SAMPLE WITHDRAWAL OF CONSENT FORM FOR FUNDRAISING

Withdrawal of Consent to the Collection, Use and Disclosure of Personal Information for Fundraising Purposes

I, _____ (**First and Last** Name) no longer wish **[Hospital]** to use the following personal information about me for fundraising purposes:

- ☐ my name and mailing address
- ☐ the following personal information: _____

(check all that apply)

Name: _____

Address: _____

_____

Signature: _____ Date: _____

Managing Contracts and Agents

Table of Contents

Managing Contracts and Agents

Key Points

- Your service providers, suppliers, employees, volunteers and others who help you carry out your duties are considered "agents" under the Act. Your agents can be internal or external to your organization.
- You may allow your agents to handle your patients' personal health information if you follow the rules in this Section.
- Your agents must comply with the rules in the Act that apply to them.
- You should ensure that your agents are informed of these rules.
    - For example, by providing staff training to internal agents, and by entering into Information Sharing Agreements with external agents.
- You must take reasonable steps to protect personal health information that you provide to your agents. For example, you should:
    - conduct effective due diligence before hiring agents,
    - include privacy protection clauses in your contracts with agents, and
    - enforce the privacy protection clauses in your contracts with agents.

Managing Contracts and Agents

The Rule

You may hire service providers, suppliers, employees and others to help you carry out your duties. When working with these individuals and organizations you may find you need to provide patients' personal health information to them. These individuals and organizations are considered to be your "agents" (as defined in the Act), and they can be internal or external to your organization. Regardless of their internal or external status, your agents must comply with the rules in the Act that apply to them.

You may allow your agents to collect, use, disclose, retain or dispose of your patients' personal health information if:

- you yourself may collect, use, disclose, retain or dispose of the information,
- your agents will collect, use, disclose, retain or dispose of the information as part of their obligations to you (through a service or supply contract, for example) and their actions are not contrary to the limits imposed by you, the Act or another law.

You should ensure that your agents are informed of their duties under the Act.

Your agents must:

- have your permission to collect, use, disclose, retain and dispose of personal health information on your behalf,
- use the information only for the stated purpose and for no other purpose except as permitted or required by any law, and
- alert you if the information they handle for you is stolen, lost, accessed by unauthorized persons, or used, disclosed or disposed of in an unauthorized manner.

You may share personal health information with your agents for a number of reasons. In addition to the reasons you describe to your patients when you collect their personal health information, additional reasons may include:

- planning or delivering programs or services, allocating resources to them, evaluating or monitoring their success, and preventing fraud or unauthorized receipt of services or benefits,

- managing risk and error,
- improving or maintaining the quality of care, programs and services,
- teaching your agents how to provide health care,
- disposing of or removing personal information from a document,
- obtaining consent (only name and contact information may be used for this reason),
- testifying in a court or other proceeding (only applies to related information),
- collecting payment or processing claims for payment for health care services,
- conducting research (if the requirements for research are followed), and
- reasons permitted or required by any Act.

What You Need To Do

You must take reasonable steps to protect personal health information that you provide to your agents.

You should:

Due Diligence	*Contracts*	*Enforcement*
• Investigate potential agents for their privacy compliance before hiring them (for organizations) • Interview potential agents with privacy compliance in mind before hiring them (for individuals)	• Include privacy protection clauses in your contracts with agents (e.g., in your third-party supply contracts with external agents or in your confidentiality agreements with internal agents)	• Enforce the privacy protection clauses in your contracts with agents

Note: The remainder of this section describes best practices for dealing with external institutional agents. The Security sections of this Toolkit describe best practices for dealing with individual agents (whether internal or external).

Due Diligence

You should investigate whether potential agents have taken steps to comply with applicable privacy laws before you hire them.

You should check whether they have:

- appointed a privacy officer,
- developed a written privacy policy,
- assessed security risks, understood legal requirements, and taken steps to address any risks,
- adopted a reasonable security standard,
- demonstrated a commitment to privacy, and
- effectively trained and sensitized staff to privacy and security related issues.

When using a Request for Proposal, you should:

- outline privacy protection requirements,
- confirm that your agents build the full cost of privacy compliance into their proposals,
    - If not, you could end up paying if a supplier needs to change technology, security, or data handling or storage practices
- ask potential agents how they plan to meet your privacy requirements and evaluate them on this plan,
    - Ask how they propose to protect personal health information from theft, loss and unauthorized access, copying, modification, use, disclosure and disposal, and how they will make sure information is accurate

- get enough information to assess and differentiate between privacy compliance plans and validate the capability and resources to comply with the plan,

    - Get as much information as you can, but do not make your questions too specific. You want potential agents' honest and accurate answers, not the answers they think you want to hear. Ask open-ended questions that do not suggest answers. For example, instead of asking whether potential agents have appointed a privacy officer, ask them to fully describe their current privacy practices. Their descriptions will let you decide whether they fully understand and are committed to privacy.

Contracts

You should make sure your agents put in place effective privacy protection practices.

When you share personal health information with your agents, you place sensitive information under your control into their hands. You have an obligation to take reasonable steps to ensure that this information continues to be protected.

Do this by writing effective contracts, and follow the Checklist for Agents Agreements.

You should review your existing contracts and, where necessary, amend them to contain appropriate privacy protection clauses. If your agents resist these amendments, call your lawyers for advice.

Enforcement

Your responsibilities do not end after you sign a contract. You should monitor whether your agents are meeting the privacy requirements in their contracts.

You should do this by:

- setting dates for your agents to report on their compliance,
- conducting on-site evaluations of your agents' privacy protections,

- holding regular meetings to discuss how current procedures are working and develop ways to remedy issues, and
- notifying agents of any changes in your own information practices and asking them to put applicable changes in place.

You should enforce the privacy requirements in your contracts. If your agents do not resolve existing problems, you may need to go to court or end the contract.

Information Sharing Agreements

If you share personal health information with others, such as external researchers or health data institutes, you should have a proper one or two-way information sharing agreement.

To ensure that your information sharing agreements provide sufficient privacy protection, follow the Checklist for Information Sharing Agreements.

Dealing with Agents Operating Outside of Ontario

The best way to make your agents comply with Ontario's law is to put Ontario's privacy requirements into your contract.

It may be difficult to ensure that your agents who operate outside of Ontario comply with Ontario privacy requirements.

- They are less likely to be familiar with Ontario's privacy requirements.
- They may claim that their compliance with other privacy requirements should suffice.
- They may not feel compelled to respect privacy laws beyond their own jurisdiction.
- The Commissioner will hold you responsible for the activities of your agents outside of Ontario.

Your contracts should bind your agents to Ontario's privacy requirements, and you can enforce the contracts against these agents outside of Ontario if need be.

Related Sections of the Act

Sections 2, 3, 4, 6(1), 7(1)(b)(ii), 10(4), 17, 37 of the Act

Section 6 of the General Regulation

Checklists, Templates and Tools

- Checklist for Agents Agreements
- Checklist for Information Sharing Agreements

CHECKLIST FOR AGENTS AGREEMENTS

Bind your agents to:

- name someone to be responsible for privacy compliance,
- only use the information you share with them as needed to fulfill the contract,
- only disclose information you or the law allows,
- put effective administrative, technological and physical safeguards in place to stop theft, loss and unauthorized access, copying, modification, use, disclosure or disposal of information that are at least as rigorous as your own and those offered to the agents' other clients,
- only give access to subcontractors that you have approved, and only enter into subcontracts that have all of the security provisions contained in your contract with them,
- educate their employees on privacy laws and policies and take reasonable steps to ensure employee compliance through staff training, confidentiality agreements and employee sanctions,
- ensure that employees who are fired or resign return all information and cannot access applications, hardware, software, network and facilities belonging to either you or the agents,
- remind exiting employees of their continued responsibility to maintain the confidentiality of the information,
- use reasonable efforts, including virus protection software, to avoid viruses, worms, back doors, trap doors, time bombs and other malicious software,
- maintain backup security and acceptable business recovery plans (including disaster recovery, data backup and alternate power),
- follow all applicable privacy laws, including the Act,
- comply with their own privacy policies,
- share their privacy policy with you and send you any updates or changes made during the term of the contract,
- refer anyone trying to access, correct or complain about their personal health information to your contact person,

- let you inspect their premises and security practices to ensure they are following the law, your contract and privacy policies,
- let you review their internal practices, books and records relating to their use and disclosure of your patients' information so you can ensure compliance,
- review security regularly and address any threats revealed,
- regularly report on compliance,
- report any security breaches or incidents to you within an agreed time,
- revoke any user's access if security is breached and on your reasonable request,
- give you a copy of your data when you ask for it,
- securely discard or return any personal health information on your request,
- comply with any sanctions for breaching the contract, including ending the contract or compensating you,
- end the contract for not following it in a significant way,
- return or destroy all information received or created in any form when the contract ends, and where this is not possible, keep the contract's privacy measures in place to protect the remaining information, and
- never deny you access to information you request because of your late or disputed payment for services.

Your contracts should also include:

- your right to go to court for an order stopping an agent from violating privacy sections of the contract and an acknowledgement that you have been irreparably harmed,
- your remedies for an agent's breach of the contract, and
- a clause making your agent responsible to you for any costs you pay because of your agent's failure to sufficiently protect your patients' information, with insurance to back the clause up

When sharing personal health information with health information network providers, you should make sure your contract requires them to give you:

- an electronic record of all accesses to the information, including the date, time and source of access,
- an electronic record of all transfers of the information, including the person who transferred the information, the person or address to whom the information was sent, and the date and time it was sent, and
- a written assessment of how the services they offer may threaten, make vulnerable or risk the security and integrity of the information, and how they impact privacy.

CHECKLIST FOR INFORMATION SHARING AGREEMENTS

To ensure that your information sharing agreements provide sufficient privacy protection:

- define all terms that may be unique to your agreement,
- define "personal health information" to include all of the information you will share,
- describe the purpose for sharing the information,
- refer to the law that allows you to collect and share the information,
- list the kind of personal health information each party will share with the other,
- identify the allowed uses for the shared information and require the other party to use the information for only those purposes,
- describe exactly how you will share the information,
- identify whether any information may be linked to or matched with other information,
- agree to verify the information received to ensure it is accurate before using it,
- set out the administrative, technological and physical safeguards needed to protect the security of the information (see the Checklist for Agent Agreements for examples of appropriate safeguards clauses),
- place necessary restrictions on disclosure,
- limit the agreement's term to ensure information will be shared for only as long as necessary,
- state how long personal health information will be kept and how it should be disposed of when the time comes, and
- describe any process for ending the agreement before the agreed upon date.

Oversight

Table of Contents

Oversight

Key Points

- The Information and Privacy Commissioner/Ontario (Commissioner) oversees compliance with the Act.
- Patients have the right to file a complaint against you with the Commissioner (for example, if they believe you have breached their privacy, or if they are not satisfied with your response to their access or correction request).
- The Commissioner responds to complaints that it receives about you, may review a complaint and may initiate a review on its own behalf.
- The Commissioner has the power to make a range of orders, where appropriate.
- A breach of privacy may entitle affected individuals to sue you for damages.
- If you are found guilty of an offence, you could be fined.
- You should implement procedures to avoid privacy breaches.
- You should implement procedures to manage any privacy breaches. These procedures must cover, at the very least, containment and notification procedures.
- You should implement procedures and make best efforts to resolve privacy complaints internally.
- The procedures that you implement, as well as your response to a privacy breach or complaint, may positively affect the final outcome of any Commissioner's review.

Privacy Breaches

What is a Privacy Breach?

A privacy breach happens when personal health information is collected, used, disclosed or disposed of in a way that does not comply with the Act.

The most common privacy breaches are:

- unauthorized collection of personal health information (information is collected without consent or legal authority),
- unauthorized disclosure of personal health information through:
  - loss (a file is misplaced),
  - theft (a laptop is stolen), or
  - mistake (a letter addressed to one person gets faxed to the wrong person), and
- unauthorized or unsecured disposal of personal health information (an unshredded file is left in the garbage).

Individuals with reason to believe that you have breached or are about to breach or compromise privacy may complain to the Commissioner. And, if the Commissioner learns of a possible privacy breach on its own, it may initiate a privacy review.

Because a complaint review is future-oriented, if a privacy breach is established, the Commissioner will help you to take the steps necessary to prevent another privacy breach from happening.

Avoiding a Privacy Breach

Adopt some or all of the following pro-active measures to prevent a privacy breach from occurring:

Requirements

- Designate a contact person.

- Inform management and staff about privacy compliance.
- Put policies and procedures in place that address privacy compliance.

Best Practices

- Identify and document roles and responsibilities needed to prevent, and when necessary manage, a privacy breach as part of a general incident management plan.
- Document information management and protection procedures and audit results so that you can avoid a privacy breach (and if necessary quickly determine the cause of a breach) and be able to demonstrate your good practices to the Commissioner.
- Determine whether your new technologies, information systems and proposed programs or policies meet basic privacy requirements.
- When in doubt, obtain advice from your lawyers.
- Consult the Commissioner's Policy and Compliance Department.

Addressing a Privacy Breach

If you learn of a privacy breach, you should take immediate action. Your first two priorities are to contain the breach and notify anyone affected.

Containment

Requirement

- Identify the extent of the privacy breach and take steps to contain it.

Best Practices

- Retrieve the hard copies of any personal health information that has been disclosed.
- Ensure that the person who was not authorized to receive the information did not make or keep copies of the information and get that person's contact information in case you need to follow up.

- Determine whether the privacy breach allows unauthorized access to any other personal health information (for example, through an electronic information system). Take all appropriate steps (for example, change passwords) to stop any further breaches.

Notification

Requirement

- Identify the people whose privacy has been breached.
- Notify (by telephone or in writing) anyone whose privacy was breached (except for any of those who do not have the right to see or obtain their own information).
- Specify what and how much personal health information was affected.
- Explain immediate and long-term steps you and others have taken to rectify the breach.
- Note down the unauthorized uses and disclosures in or linked to the affected personal health records.

Additional Steps

Best Practices

- Identify the person who will manage the breach and the person who will communicate with the public about the breach. Tell staff who will play these roles. (The same person might play both roles in a smaller organization.)
- Tell staff not to communicate with the public — that is the communicator's role. This is especially important when it comes to communicating with the media.
- Make an assessment of the personal health information you hold and how you use and disclose it so that you can see what information might be involved in a breach.

  See the Sample Inventory of Personal Health Information for an example.
- Notify management, staff, your contact person and your lawyers (if appropriate) of the privacy breach.

- If the breach is a serious one, or raises questions of public concern, investigate what happened to:
  - ensure immediate containment and notification requirements are addressed,
  - identify the circumstances surrounding the breach, and
  - review whether your policies and procedures adequately protect personal health information.
- Address the situation systemically. In some cases, program- or institution-wide procedures may warrant review (for example, a misdirected fax may prompt review of your faxing process).
- Inform the Commissioner's registrar of the privacy breach and work constructively with the Commissioner's staff.
- Let the Commissioner know your findings and work together to make needed changes.
- Train management and staff appropriately on privacy compliance.

Reviewing a Privacy Complaint

Depending on the circumstances, when the Commissioner reviews a complaint it may:

- ensure all containment and notification issues have been addressed,
- discuss the complaint with the parties and obtain any relevant information,
- interview individuals involved with the privacy breach and others who can provide relevant information,
- seek and consider your representations on the issues raised by the privacy complaint,
- ask you to report any actions you have taken,
- review a copy of the personal health information involved,
- research its precedents,
- discuss options for resolution,

- recommend changes to current privacy policies, procedures and relevant documents,
- issue a report or order at the end of the review, and
- make recommendations on the privacy implications of any matter that is the subject of the review.

The Commissioner's Role

The Information and Privacy Commissioner/Ontario ("Commissioner") oversees privacy and freedom of information legislation in Ontario, including the Act. Under the Act, the Commissioner:

- responds to privacy complaints,
- initiates privacy reviews,
- authorizes certain information collection practices, where appropriate,
- educates and communicates with the public about health privacy,
- researches issues affecting health privacy, and
- offers comments advice on current or proposed information practices, on request.

The Commissioner's Powers

Responding to Privacy Complaints

Generally, the Commissioner will inform you of any complaints it receives about you, although you may not receive notice where, for example, the Commissioner dismisses the complaint at an early stage of the process.

If the Commissioner decides a formal review is warranted, the Commissioner may ask:

- those who complained what other steps they have taken to resolve their concerns,
- those who complained to try to resolve their complaint directly with you by a certain date, and
- a mediator to facilitate resolving the complaint by a certain date.

If the complaint is not resolved, the Commissioner may decide to review the complaint. The Commissioner will let you know if it plans to review a complaint.

The Commissioner may decide not to review the complaint if:

- you have dealt with the complaint adequately,
- the complaint should be dealt with in another manner,
- the complaint was made too late,
- the person who complained had insufficient personal interest in the complaint,
- the complaint was frivolous, vexatious or made in bad faith, or
- for any other reason the Commissioner considers proper.

If the Commissioner decides not to review the complaint, it will tell the complainant why.

Initiating Privacy Reviews

The Commissioner may (on its own initiative) conduct a privacy review of any matter where there are reasons to believe you may not be complying with the Act. The Commissioner will tell you if it intends to conduct a review that affects you or your operations.

Conducting Privacy Reviews

When conducting a review, the Commissioner will follow its own established rules of procedure and receive any information it considers appropriate and relevant to the complaint.

In certain circumstances, the Commissioner may also:

- inspect your business (without a warrant or court order),

- inspect your residence (with a warrant or your consent),
- review your books, records, information, information practices and other materials, and
- compel others to provide information.

The Commissioner needs your patients' consent before reviewing their personal health information that you hold. However, if:

- the Commissioner believes that it must review the information to complete the review,
- the public interest justifies reviewing the information without consent,
- the Commissioner places conditions or restrictions on the review that the Commissioner determines is warranted, and
- the Commissioner tells you in writing of its decision to review information without consent, and its reasons for and conditions and restrictions on, this review,

then, consent is not necessary.

Result of the Review

Depending upon the nature of the complaint and the result of its review, the Commissioner may order you to:

- give access to the requested record to the person who complained,
- make the correction that the person who complained asked for,
- perform a duty imposed by the Act,
- stop collecting, using or disclosing personal health information in breach of the Act or a contract,
- dispose of records of personal health information collected, used or disclosed in breach of the Act or a contract (so long as doing so would not negatively affect any individual's health care),
- change, stop or never start a particular information practice that breaches the law, or

- put an information practice in place to comply with the law.

The Commissioner may also order those acting on your behalf or with you (your agents) to take action to ensure you comply with its order against you.

The Commissioner may make recommendations on how anything subject to the review affects privacy.

The Commissioner will provide a copy of any comments, recommendations or an order made, together with the terms and reasons, to:

- you,
- the complainant (if there is one),
- other persons to whom the order is directed,
- the body or bodies that regulate you,
- any person whom the Commissioner considers appropriate.

If the Commissioner makes no order after its review, the Commissioner will tell both you and the person who complained why.

You may appeal the Commissioner's orders (except access and correction orders) to the court on questions of law. The court may order the Commissioner to take actions that the Commissioner is authorized to take under the Act, confirm the Commissioner's order or, if necessary, vary or set the order aside. Once all avenues of appeal have been exhausted, or if no appeal is made, an order may be filed with the court, making it an enforceable judgment of the court.

If new facts come to light following the Commissioner's order, the Commissioner may cancel or change its order or make a further order, even if the original order has been filed with the court. All affected parties will receive notice of the new order. You or other parties may appeal the new order.

You may ask the court to review an order concerning access or correction by way of an application for judicial review.

Offence and Sanctions

If you violate the law, you may face:

- a Commissioner's order,

- a fine for an offence, and/or
- a lawsuit for damages.

Note: Not all privacy breaches are subject to fines.

It is an offence for you to:

- wilfully collect, use or disclose personal health information in breach of the law,
- dispose of a personal health record to evade an access request,
- dispose of a personal health record in a manner that is not secure,
- wilfully obstruct or mislead the Commissioner in performing its duties under the Act,
- wilfully fail to comply with a Commissioner's order, or
- discipline or disadvantage an employee for trying to comply with the Act.

If prosecuted and convicted of an offence:

- a hospital or physician could be fined up to $250,000 or $50,000 respectively, and
- the hospital's officers, members, employees or other agents who authorized or could have prevented the offence may be fined $50,000, whether or not the hospital itself is prosecuted or convicted.

A breach of privacy may entitle affected individuals to sue you for damages for:

- actual harm a privacy breach caused, or
- mental anguish (up to $10,000) where wilful or reckless behaviour caused the breach.

Related Sections of the Act

2, 3, 4, 12(2), 12(3), 16(2), 17(3), 54(8), 56-72

Checklists, Templates and Tools

- Sample Inventory of Personal Health Information
- Commissioner Contact Information
- Decision Tree – Responding to Complaints about Privacy Breaches

SAMPLE INVENTORY OF PERSONAL HEALTH INFORMATION

Name	Information	Info Steward	Location	Backup Copies	Security	Retention	Notes
Master Patient Health Records	Patient info: - Name - Contact info - Health # - Family info - Health history	John Q. Deere	UNIX server at College Street	Offsite storage	Password protected via EHR application Encrypted in storage	Archive after ● years	Accessed via EHR application

COMMISSIONER CONTACT INFORMATION

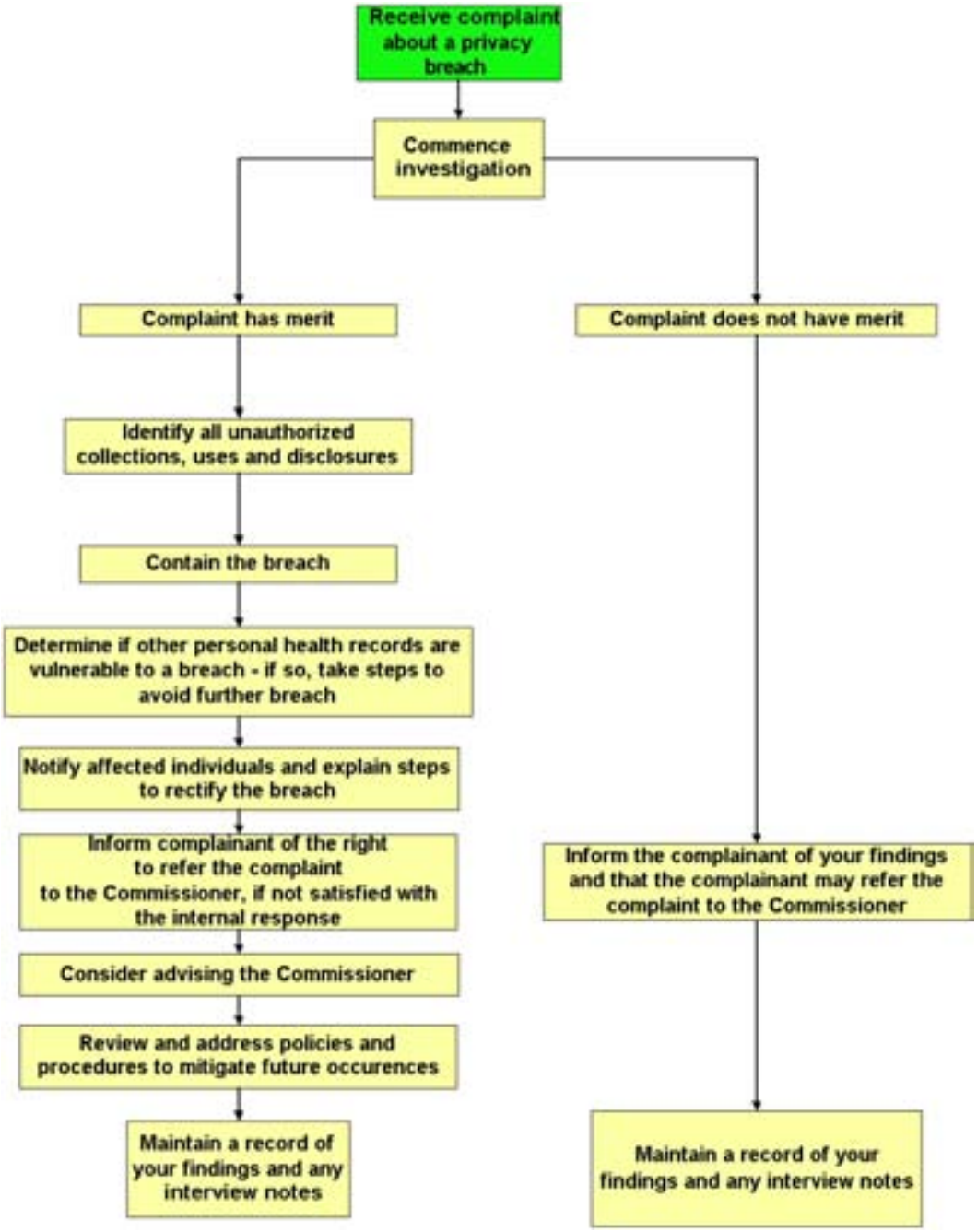
The Commissioner can be reached at:

Telephone: (416) 326-3333

Email: info@ipc.on.ca

Website: www.ipc.on.ca

DECISION TREE - RESPONDING TO COMPLAINTS ABOUT PRIVACY BREACHES



Glossary

Glossary

This glossary explains the meaning the following terms have when used in this Toolkit.

A

"Access" means patients' ability to examine or obtain information about themselves.

"Act" means the *Personal Health Information Protection Act, 2004* and the regulations made under it.

"Agent" means any person that a health information custodian authorizes to act for it to deal with other people's personal health information, whether or not the agent has authority to bind the custodian, is employed by the custodian, or is being paid.

"Attorney for personal care" means someone who can legally act for another person because they have a power of attorney for personal care under the *Substitute Decisions Act*.

"Attorney for property" means someone who can legally act for another person because they have a continuing power of attorney for property under the *Substitute Decisions Act*.

"Audit" means to conduct an independent review and examination of system records, activities and practices to test the adequacy and effectiveness of data security and data integrity procedures, to ensure compliance with health records policy and operational procedures.

"Authentication" means the procedure for establishing the identity of a user.

"Authorization" means the procedure to establish which resources and information a user may access and what actions they are allowed to perform on those resources such as reading, updating, creating or deleting information.

Glossary

B

"Biometrics" means the use of methods of authenticating or verifying an individual's identity based upon a physical or behavioural characteristic, such as retina patterns or skin characteristics.

"Board" means the Consent and Capacity Board created under the *Health Care Consent Act*.

C

"Capable" means mentally able to make decisions for oneself.

"Capacity" means the mental ability to make decisions for oneself.

"Collect" means to gather, receive or obtain personal health information in any way and from anyone.

"Collection" means the gathering, receiving or obtaining of personal health information in any way and from anyone.

"Commissioner" means the Information and Privacy Commissioner/Ontario appointed by statute.

"Conditional consent" means a patient's consent to the collection, use or disclosure of personal health information on which the patient has placed a restriction. See the Consent section for additional information on conditional consent.

"Contact Person" means the person designated to assist you in meeting your privacy obligations and to respond to patient inquiries about privacy-related matters.

D

"De-identified information" means health information from which personally identifying information has been removed, and for which no means exists to re-identify patients.

"Disclose" means to release or make personal health information available to another person, organization or health information custodian; it does not mean to use the information.

"Disclosure" means the release or making available of personal health information to another person, organization or health information custodian; it does not mean the use of the information.

E

"Encryption" means using recognized techniques to transform plain electronic information into an unintelligible form that requires a special key in order to transform it back into the intelligible format.

F

"Firewall" means a combination of hardware and software, used to protect a network from unauthorized access, intrusion or traffic.

G

"Guardian of property" means a person appointed to act as guardian of another person's property, or a statutory guardian of property under the *Substitute Decisions Act*.

"Guardian of the person" means a person appointed to act as guardian of another person under the *Substitute Decisions Act*.

H

"Health card" means a card provided to a person by the Ontario Health Insurance Plan to identify the card holder as entitled to health care benefits in Ontario.

"Health care" means treating, observing, examining, assessing or caring for a person for a health-related purpose and includes to:

- diagnose, treat or maintain the person's physical or mental condition,
- prevent disease or injury,
- promote health, or
- provide a service as part of palliative care.

Health care includes compounding, dispensing or selling drugs, devices, equipment or any other item prescribed to an individual. It also includes any community service a service provider performs – see the *Long-Term Care Act*.

"Health care practitioner" means:

- a member of any profession that the *Regulated Health Professions Act* covers who provides health care,
- anyone registered as a drugless practitioner under the *Drugless Practitioners Act* who provides health care,
- a member of the Ontario College of Social Workers and Social Service Workers who provides health care, and
- anyone else who primarily provides health care for which they get paid.

"Health information custodian" means any person or organization who controls other people's personal health information as part of their role as:

- a health care practitioner or operator of a group practice of health care practitioners,
- a service provider who provides a community service under the *Long-Term Care Act*,

- a community care access corporation under the *Community Care Access Corporations Act*,
- someone who operates one of the following facilities, programs or services:
  - a hospital under the *Public Hospitals Act*, a private hospital under the *Private Hospitals Act*, a psychiatric facility under the *Mental Health Act*, an institution under the *Mental Hospitals Act* or an independent health facility under the *Independent Health Facilities Act*,
  - an approved charitable home for the aged under the *Charitable Institutions Act*, a placement co-ordinator under the *Charitable Institutions Act*, a home or joint home under the *Homes for the Aged and Rest Homes Act*, a placement co-ordinator under the *Homes for the Aged and Rest Homes Act*, a nursing home under the *Nursing Homes Act*, a placement co-ordinator under the *Nursing Homes Act* or a care home under the *Tenant Protection Act*,
  - a pharmacy under the *Drug and Pharmacies Regulation Act*,
  - a laboratory or specimen collection centre under the *Laboratory and Specimen Collection Centre Licensing Act*,
  - an ambulance service under the *Ambulance Act*,
  - a home for special care under the *Homes for Special Care Act*, or
  - a centre, program or service for community health or mental health whose primary purpose is to provide health care,
- an evaluator under the *Health Care Consent Act* or an assessor under the *Substitute Decisions Act*,
- a medical officer of health or a board of health under the *Health Protection and Promotion Act*,
- the Minister or Ministry of Health and Long-Term Care, and
- any other person described as a health information custodian under the regulations to the Act with custody or control of personal health information as part of performing powers, duties or work.

"Health number" means the number that OHIP assigns to an insured person under the *Health Insurance Act*.

Glossary

I

"Identifying information" means any information that identifies an individual or that one could reasonably foresee might be used either on its own or with other information to identify an individual.

"Incapable" means mentally unable to make decisions for oneself.

"Incapacity" means the mental inability to make decisions for oneself.

"Individual" means any living or deceased person about whom personal health information was or will be collected or created.

"Information practices" means a health information custodian's policies concerning when, how and why the health information custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and the administrative, technological and physical safeguards and practices maintained to protect personal health information.

"IT" means information technology and refers to any electronic computing or network technology, including both hardware and software.

"IT infrastructure" means the collective set of information technology tools and technologies, especially networks and servers, that an organization uses to support its operations.

L

"Lock box" is not defined in the Act. Lock box describes the limits that patients can place on the disclosure of their personal health information. See the Managing Health Information section for additional information on lock boxes.

"Logical security" means software and procedural measures designed to provide protection of IT resources and electronically stored information against deliberate and accidental logical threats, including measures such as passwords and firewalls.

M

"Malicious software" means software designed to corrupt, destroy, take over or deny availability to information technology resources. Malicious software includes viruses, worms, Trojan Horses, logic bombs and other types of harmful code.

"Minister" means the Minister of Health and Long-Term Care.

N

"Need to know" means the principle that a staff member should have access only to the personal health information needed to perform a particular function.

P

"Partner" means one of two persons who have lived together for at least one year in a close personal relationship of primary importance to both people in the relationship.

"Person" means an individual person, a partnership, an association and any other entity.

"Personal health information" means oral or recorded identifying information about someone that relates to:

- a person's physical or mental health or family health history,
- health care an individual receives, including who provided the health care,
- a plan of service for an individual under the *Long-Term Care Act*,
- an individual's eligibility for health care payments or the payments made for an individual's health care, and
- an individual's donation of any body part or bodily substance or anything derived from testing or examining a donated body part or bodily substance.

Personal health information also includes:

- an individual's health number,
- anything that identifies an individual's substitute decision-maker, and
- anything that identifies an individual and that is contained in a personal health record.

Personal health information does not include records maintained for human resources purposes.

"Physical security" means physical measures designed to provide physical protection of resources against deliberate and accidental threats, to prevent unauthorized access to equipment, installations, documents, files and records, including measures, such as door locks, camera, passcard readers, safes and security guards taken to control access to restricted areas.

"Privacy" means the right of individuals to determine for themselves when, how and to what extent personal information about the individuals is communicated, and to be secure from unauthorized use or disclosure of their personal information.

"Proceeding" means any proceeding before a court, tribunal or committee of a professional regulatory body.

"Provincially funded health resource" means any health-related or prescribed service, subsidy or other benefit that the Ontario government wholly or partially funds.

R

"Record" means an information record in any form or media, including written, printed, photographic or electronic form, but excluding computer programs and other mechanisms that produce a record.

"Relative" means one of two people related to each other by blood, marriage or adoption.

"Research" means a systematic investigation to develop or establish principles, facts or knowledge including developing, testing and evaluating research.

"Researcher" means anyone who conducts research.

"Research Ethics Board" means a board established to approve research plans under the Act.

S

"Security" means the physical, technological and administrative protective measures and techniques that are designed to ensure that personal health information remains confidential, available and uncompromised. This includes measures such as encryption, passwords, and firewalls designed to prevent unauthorized access to information, to protect the integrity of computing resources, and to limit the potential damage that can be caused by unauthorized access.

"Spouse" means one of two people whose relationship is recognized under Ontario law and includes married people and people living together in common law relationships.

"Substitute decision-maker" means a person that the Act authorizes to give consent on another's behalf to the collection, use or disclosure of the other person's personal health information.

T

"Threat risk assessment" means a structured process to evaluate security threats, vulnerabilities, probabilities and business impact to an organization's critical assets.

U

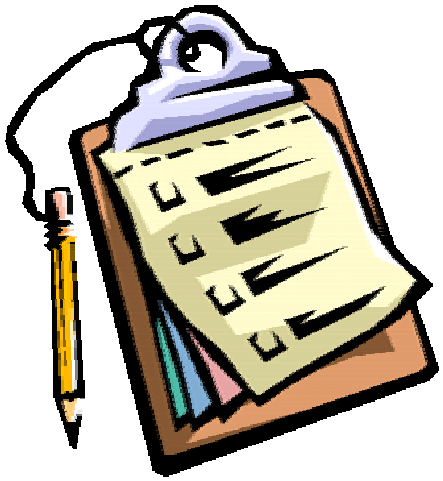
"Use" means to handle or deal with personal health information but does not mean to disclose personal health information.

"User" means a person authorized to use specific resources of an organization's IT infrastructure. A user usually accesses these resources through a User ID and a password.

V

"Virus" means a piece of malicious computer software. Anti-virus software is software designed to detect and prevent computer viruses from causing harm.

Appendix of Forms



Contents

NOTE TO USER: When you use this Statement, you must ensure that you have included all of your proposed uses and disclosures. If you use or disclose a patient's personal health information, without the patient's consent, in a manner that is not described on the Statement, you must: (a) inform the patient of this as soon as possible unless the patient does not have a right of access to their personal health record, and (b) make and keep a note of the use or disclosure in or linked to the affected patient's personal health record.

SAMPLE WRITTEN STATEMENT OF INFORMATION PRACTICES

Collection of Personal Health Information

We collect personal health information about you directly from you or from the person acting on your behalf. The personal health information that we collect may include, for example, your name, date of birth, address, health history, records of your visits to **[the Hospital]** and the care that you received during those visits. Occasionally, we collect personal health information about you from other sources if we have obtained your consent to do so or if the law permits.

Uses and Disclosures of Personal Health Information

We use and disclose your personal health information to:

- treat and care for you,
- get payment for your treatment and care (from OHIP, WSIB, your private insurer or others),
- plan, administer and manage our internal operations,
- conduct risk management activities,
- conduct quality improvement activities (such as sending patients satisfaction surveys),
- teach,
- compile statistics,
- fundraise to improve our healthcare services and programs,
- comply with legal and regulatory requirements, and
- fulfil other purposes permitted or required by law.

Your Choices

You may access and correct your personal health records, or withdraw your consent for some of the above uses and disclosures by contacting us (subject to legal exceptions).

Important Information

- We take steps to protect your personal health information from theft, loss and unauthorized access, copying, modification, use, disclosure and disposal.
- We conduct audits and complete investigations to monitor and manage our privacy compliance.
- We take steps to ensure that everyone who performs services for us protect your privacy and only use your personal health information for the purposes you have consented to.

How to Contact Us

Our privacy contact person is ●.

For more information about our privacy protection practices, or to raise a concern you have with our practices, contact us at:

[Address, fax, email, telephone number and website]

You have the right to complain to the Information and Privacy Commissioner/Ontario if you think we have violated your rights. The Commissioner can be reached at:

[Address, fax, email, telephone number and website]

NOTE TO USER: This Sample Consent Form provides a sample list of purposes for the collection, use and disclosure of personal health information where *express consent* is required under the Act. You should consider whether your intended purpose for the collection, use and disclosure of personal health information requires express consent and amend this form to include all such purposes. If you choose to rely on express oral consent, no such form is needed.

SAMPLE CONSENT FORM

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

I, _____, have reviewed the [Hospital]'s written statement concerning the collection, use and disclosure of personal health information.

I understand that the [Hospital] is seeking my consent for it to collect, use and/or disclose my personal health information from me or from the person acting on my behalf to:

- ☐ teach outside the **[Hospital]**,
- ☐ fundraise for the **[Hospital]**'s charitable activities, using more than my name and mailing address,
- ☐ _____, and
- ☐ _____

I understand that the **[Hospital]** will only collect, use and disclose my personal health information with my consent **(as set out in its privacy policy)** unless a particular collection, use or disclosure is permitted or required by law without my consent.

I also understand that I can refuse to sign this consent form. I can also withdraw my consent any time by writing to ●

I hereby authorize **[Hospital]** to collect, use and disclose my personal health information for the purposes that I have checked-off above.

Name: _____

Address: _____

Signature: _____ Date: _____

FOR INTERNAL OFFICE USE ONLY

Patient ID No. _____

SAMPLE WITHDRAWAL OF CONSENT FORM

Withdrawal of Consent

I, _____, wish to withdraw my consent to any further use or disclosure by **[Hospital/Physician name]** of my personal health information for: (Please check all that apply)

- ❑ Teaching outside the **[Hospital]**
- ❑ Fundraising, using more than my name and mailing address.
- ❑ _____, and
- ❑ _____.

I wish to place the following conditions on any further use or disclosure of my personal health information:

_____

_____

(Please specify conditions)

This withdrawal of consent does not have retroactive effect nor does it affect the uses and disclosures of personal health information collected by **[Hospital/Physician Name]** where the uses and disclosures are permitted or required by law without consent.

Name: _____

Address: _____

Signature: _____ Date: _____

SAMPLE CONFIDENTIALITY AGREEMENT

NOTE TO USER: Modify this sample agreement to suit your institution and your needs. Review with your lawyers before releasing.

I acknowledge that I have read and understood the **[●]** policies and procedures on privacy, confidentiality and security.

I understand that:

- all confidential and/or personal health information that I have access to or learn through my employment or affiliation with **[●]** is confidential,
- as a condition of my employment or affiliation with **[●]**, I must comply with these policies and procedures, and
- my failure to comply may result in the termination of my employment or affiliation with **[●]** and may also result in legal action being taken against me by **[●]** and others.

I agree that I will not access, use or disclose any confidential and/or personal health information that I learn of or possess because of my affiliation with **[●]**, unless it is necessary for me to do so in order to perform my job responsibilities. I also understand that under no circumstances may confidential and/or personal health information be communicated either within or outside of **[●]**, except to other persons who are authorized by **[●]** to receive such information.

I agree that I will not alter, destroy, copy or interfere with this information, except with authorization and in accordance with the policies and procedures.

I agree to keep any computer access codes (for example, passwords) confidential and secure. I will protect physical access devices (for example, keys and badges) and the confidentiality of any information being accessed.

I will not lend my access codes or devices to anyone, nor will I attempt to use those of others. I understand that access codes come with legal responsibilities and that I am accountable for all work done under these codes. If I have reason to believe that my access codes or devices have been compromised or stolen, I will immediately contact the **[●]**.

Name (Please Print)	**Signature**	**Date**

SAMPLE CONSENT TO DISCLOSE PERSONAL HEALTH INFORMATION FORM

I _____ hereby authorize _____
(Name of hospital/physician's office)

to disclose the following personal health information:

_____

_____
(Description of personal health information to be disclosed and dates of contact/hospitalization)

to _____

_____
(Name and address of person/agency requesting information)

from the records of _____
(Name of Patient) **(Birth date)**

Mailing Address of Patient: _____

_____

I understand that this personal health information is to be used **only** by the recipient for the purposes of:

_____

_____

Date: _____

I hereby waive any and all claims against **[insert name of hospital/physician's office]** in connection with the disclosure of this personal health information.

Witness: _____ Signed by: _____
(Patient or Substitute Decision-Maker)

Date: _____ _____
(Relationship to the Patient)

SAMPLE FORM TO REQUEST ACCESS TO PERSONAL HEALTH RECORD

Information and Instructions

We will provide you with access to your personal health record, unless a legal exception applies. We will review all health record access requests, and will make every effort to respond to your request in a timely fashion. Please complete Parts A and B of this Form. Part C is for our internal use. For information about our privacy protection practices, contact ● at: **[Address, fax, email and telephone number.]**

PART A: REQUESTOR INFORMATION

Patient Contact Information:

Last Name _____ First Name _____ Initials _____

Mailing Address _____

Telephone Number _____ Date of Birth _____

Hospital ID Number _____

If you are a substitute decision-maker, your contact information:

Last Name _____ First Name _____ Initials _____

Mailing Address _____

Telephone Number _____

Note: Include copies of documents that provide your authority as a substitute decision-maker.

PART B: ACCESS REQUEST

1. Please describe what you need and include details that will help us locate the record (e.g., dates, name of healthcare provider, etc.).

_____

_____

2. How would you prefer to access this information? Please check off:

☐ Receive hard copies of originals
☐ Receive electronic copies of originals (please supply storage medium)
☐ Examine originals in the facility

Signature _____ Name (print) _____ Date _____

PART C: RESPONSE TO ACCESS REQUEST (For Internal Use Only)

1. Information Regarding Receipt and Initial Review of Request

_____
Date Request Received

2. Information Regarding Response

_____
Date Response Issued

☐ Access request granted
☐ Access request not granted
☐ Access request granted in part

If complete access request was not granted, reason for refusing the request/part of the request.

_____

3. Information Regarding Extension

If an extension to the access request response was required, please indicate:

Date of Extension	Reason for Extension	Date Patient Notified

4. Processed by:

Signature	Name (print)	Title

SAMPLE LETTER FOR EXTENSION TO COMPLY WITH REQUEST

[Name and Address of Health Care Facility]
XXX Street
City/Town, Ontario
ABC 123

Date

Dear Sir/Madam,

RE: Request for Access to Personal Health Record of [Patient's Name]

Health Record #:

An extension of _____ days is required to address your request to access the personal health record of the individual named above. While every effort is made to retrieve the information requested, this extension is required for the following reason:

[Reason for extension]

If you have any concerns or questions please contact _____ (Contact Person). If they are unable to resolve your concerns, you may file a complaint with the Information and Privacy Commissioner/Ontario, who may be contacted at:

[Contact information for the Information and Privacy Commissioner/Ontario]

Sincerely,

_____

[Name, Title]

SAMPLE REFUSAL OF ACCESS LETTER

[Name and Address of Health Care Facility]
XXX Street
City/Town, Ontario
ABC 123

Date

Dear Sir/Madam,

RE: Request for Access to Personal Health Record of [Patient's Name]

Your request for access to the personal health record has been declined for the following reason:

[Reason for declining request]

If you have any questions or concerns please contact _____ (Contact Person). If we are unable to resolve your concerns, you may contact the Information and Privacy Commissioner/Ontario, who may be contacted at:

[Contact information for the Information and Privacy Commissioner/Ontario]

Sincerely,

_____

[Name, Title]

SAMPLE REQUEST FORM FOR CORRECTION TO PERSONAL HEALTH RECORD

Information and Instructions

We will correct health record information if it is demonstrated, to our satisfaction, that the record is not correct or complete for the purpose for which we collect, use or disclose the information. We will make every effort to respond to your request in a timely fashion. Please complete Parts A and B of this Form. Part C is for our internal use. For information about our privacy protection practices, contact **[●]** at: **[Address, fax, email and telephone no.]**

PART A: REQUESTOR INFORMATION

Patient Contact Information:

Last Name _____ First Name _____ Initials _____

Mailing Address _____

Telephone Number _____ Date of Birth _____ Hospital ID Number _____

If you are a substitute decision-maker, your contact information:

Last Name _____ First Name _____ Initials _____

Mailing Address _____

Telephone Number _____

Note: Include copies of documents that provide your authority as a substitute decision-maker.

PART B: CORRECTION REQUEST

1. List or attach the correction requested, with reasons for the correction.

Requested Correction	**Reasons for Correction**

2. How do you wish to receive notice of the correction (in writing, by telephone)?

_____

3. Would you like us to give notice of the correction, to the extent reasonably possible, to others to whom we have disclosed the incorrect information? (We will only do so if this notice will affect your health care or otherwise benefit you.)

☐ Yes
☐ No

Signature	Name (print)	Title

Date

PART C: CORRECTION REQUEST RESPONSE (For Internal Use Only)

☐ Correction made
☐ Correction not made
☐ Refusal letter (with reasons) sent
☐ Statement of Disagreement attached to record
☐ Date of Response _____

1. List names, contact information and comments of any individuals consulted

2. If correction was not made, provide reasons:

3. If an extension to the correction request response was required, please indicate:

Date of Extension	**Reason for Extension**	**Date Patient Notified of Extension**

4. Notice of correction provided to others to whom incorrect information was disclosed. List names:

5. Processed by:

Signature	Name (print)	Title

REB File No.:
Date:

SAMPLE APPLICATION TO RESEARCH ETHICS BOARD

A. GENERAL INFORMATION

PRIMARY INVESTIGATOR

Name	Signature
Dept./Div.	Position
Qualification:	Email Address

CO-INVESTIGATOR

Name	Signature
Dept./Div.	Position
Qualification:	Email Address

CO-INVESTIGATOR

Name	Signature
Dept./Div.	Position
Qualification:	Email Address

OTHER RESEARCH TEAM MEMBERS WHO ARE <u>NOT</u> CO-INVESTIGATORS Please type names, roles and qualifications (signatures not needed)

B. DETAILS OF PROJECT

1. Project Title _____

2. Is this project funded? _____

   ☐ NO

   ☐ YES

3. Sponsor _____

4. Duration of Funding: from __/__/__ to __/__/__

5. Conflict of Interest Declaration – Do you have any conflicts of interest (actual, apparent, perceived or potential) relating to this project?*

   ☐ NO

   ☐ YES

   Description of conflict of interest _____

   Mandatory Signature _____

   (Application will be returned without signature)

   *Conflicts of interest include but are not limited to the following situations and also must be disclosed under institutional policy for review: If you or any of the involved research team members or your/their dependants have:

   (1) employment or consulting arrangements and/or a financial interest in the sponsor of the study, or with proposed subcontractors, vendors or collaborators; or

   (2) a financial interest in the subject of the study.

6. Protocol:

   a) *Nature*

   b) *Objectives*

   c) *Methods*

d) *Statistical Analysis*

e) *Anticipated Public or Scientific Benefit*

f) *Duration of Research*

g) *Foreseeable Harms and Benefits of Research (describe how harms will be addressed)*

C. INFORMATION REQUESTED

1. What patient information do you require?

_____

_____

2. What patient information source are you accessing?

☐ Health Records Clinic/Office Files	Specify which
☐ Electronic Database	Specify which
☐ Outside Institution	Specify which
☐ Other	Specify which

3. Proposed number of research subjects _____

4. Are you requesting information that identifies or potentially identifies individuals?

☐ NO
☐ YES

If yes, explain why you cannot use anonymized or aggregate information:

_____

_____

5. Have you obtained consent from the individuals to collect and use the identifying information on this project?

☐ YES Attach a sample consent form

☐ NO

If no, explain why

_____

_____

6. What security measures will be in place to protect the information during transmission?

_____

_____

D. INFORMATION LINKAGE

1. Does your project involve linking any information from this request to other information?

☐ NO
☐ YES

If yes,

Describe what information is to be linked:

_____

_____

Describe what type of linkage is required:

_____

_____

Describe the rationale for this linkage:

_____

_____

2. Have you received approval from the other information sources including division/department head authorization to conduct this linkage?

☐ NO

☐ YES Please attach the approval(s)

3. Will the information be retained in linked form?

☐ NO

☐ YES

4. When will the information be de-identified after the linkage?

_____

_____

E. DISSEMINATION OF ANALYSIS AND/OR REPORTS:

1. How do you plan to disseminate and/or publish the results of your analyses?

_____

_____

2. What is the expected date of dissemination and/or publication?

_____

F. DISCLOSURE AVOIDANCE PRACTICES

1. How will you ensure that information will be aggregated prior to disclosure, to the level required in the information sharing agreement, confidentiality agreement, privacy policy and other applicable policies and procedures?

_____

_____

_____

2. Attach information collection form or list of fields (mandatory: application will be returned if this information has not been included)
Please note that the content of the form should be adequate to answer the research questions.

3. Are any sensitive issues raised in this study or its publication (e.g. HIV status, mental health status, subjects identifiable, pedigrees, other)

☐ NO

☐ YES Please specify _____

G. SECURITY AND ACCESS

1. The information obtained from the records described above will be used for the outlined research purposes only:

☐ NO If no, a separate request must be submitted
☐ YES

2. List all of the persons who will have access to the records in an individually recognized form for the research purpose described and why they need this access: (name and role in research)

_____

_____

3. Have all these persons signed confidentiality agreements?

☐ NO

☐ YES If no, please indicate when agreement will be signed

_____

_____

H. SECURITY MEASURES

1. Describe how you will keep information secure

☐ Premises will be locked except when one or more of the individuals named in E1(b) are present

☐ Access to the premises will be controlled (passcards, security clearances etc.)

☐ Access to the information will be restricted to the research team by:

☐ Patient code ☐ Files/Folders password ☐ Computer password

Please provide name of password software_____

☐ Other computer security methods that prevent unauthorized access will be used

☐ Encryption ☐ Firewalls ☐ Identifying Information Scrambled/De-linked

Other (Describe):_____

☐ Staff will be trained regarding privacy

☐ Staff will sign a confidentiality agreement

☐ Other, explain

_____

_____

2. Will information remain within the institution?

☐ NO

☐ YES If no, please indicate why and how information will be exported outside

_____

_____

3. Will system files be backed up automatically?

☐ NO
☐ YES

If yes, please specify provisions that would be made for a private drive that cannot be accessed by anyone other than your research team, or that could not be backed up by computer support staff within your organization:

_____

_____

All original personal health records received from ● must be returned to ● and all copies of personal health records that were made or received must be destroyed in accordance with the information sharing agreement.

I certify that the information reported here is accurate and that the personal health information will not be used for future projects without prior approval of a research ethics board.

Primary Investigator Signature	Date
Division/Department Head Signature of Approval	Date

Do you plan on accessing information from another division/department?

☐ NO
☐ YES If yes, authorization from the division/department head is requested

Signature of Approval	Date

In making this request, I acknowledge that failure to comply with the terms and conditions of the information sharing agreement is cause for termination of the agreement and, where applicable, a complaint to the Information and Privacy Commissioner/Ontario.

Date	Signature of Requestor

Research Ethics Board for Retrospective Research

Signature of REB Chair	
Date of Approval	Approval Expires
Level of Continuing Review:	

SAMPLE CONSENT FORM FOR STUDY PARTICIPANT

Note to User: This Sample Consent Form is intended to be used for retrospective research. It is not appropriate to use it for clinical trials.

Study Title: ●

Primary Investigator: ●

Sponsor: ●

Background: **[Insert details about the study.]**

What is involved? ●

Benefits and Risks: ●

Voluntary: Participation in this study is completely voluntary. You can refuse to sign this consent form and to participate in the study. You can also withdraw your consent any time by writing to ●. Your care at ● will not be affected by your decision.

Confidentiality: **[Insert details about collection, use, disclosure, storage and disposal of personal health information.]**

You have had this study explained to you and had an opportunity to ask questions. You have been given a copy of this Consent Form. If you have any additional questions about the study, please contact ● at ●. If you have any additional questions about your privacy, please contact ● at ●.

Participant Consent

I agree to participate in this study.

I also permit ● to collect, use and disclose health information about me for the purposes of this study.

Name of Participant (print)	Signature of Participant
Investigator's Signature	Signature of Substitution Decision-Maker (if required)
Date	

SAMPLE CONSENT FORM FOR FUNDRAISING

Consent to the Collection, Use and Disclosure of Personal Information for Fundraising Purposes

We may use personal **[demographic]** information about you, including your name and mailing address, in order to contact you to support our fundraising programs. We may also share this information with **(our hospital foundation)**, which will contact you on our behalf. By signing below, you permit us to contact you with information on our fundraising campaigns at a later date.

You can refuse to sign this consent form. You can also withdraw your consent any time by writing to ●. Your refusal or withdrawal of consent will in no way affect the care or treatment that you receive at **[Hospital]**.

Patient Consent

I, _____ authorize **[Hospital]** to collect, use and disclose.
(First and Last Name)

☐ just my name and mailing address
☐ my name, mailing address and the following personal information.

_____ _____

[Note to User: Consider inserting the personal information you would like to use for fundraising purposes, such as email address, telephone number, etc.]

for use in fundraising relating to the **[Hospital]**'s charitable activities. I understand that you might share information about me with the hospital foundation.

Name _____ _____

Address: _____ _____

_____ _____

Signature _____ Date _____

FOR INTERNAL OFFICE USE ONLY

Patient ID No:

SAMPLE WITHDRAWAL OF CONSENT FORM FOR FUNDRAISING

Withdrawal of Consent to the Collection, Use and Disclosure of Personal Information for Fundraising Purposes

I, _____ no longer wish **(Hospital)** to use the
(First and Last Name)

following personal information about me for fundraising purposes:

- ☐ my name and mailing address
- ☐ the following personal information.

_____
(check all that apply)

Name: _____

Address: _____

_____

Signature: _____ Date: _____

Diagnostic Tool

Table of Contents

Diagnostic Tool

Overview

Purpose

This Diagnostic Tool is designed to help you identify areas you may need to work on to meet your privacy obligations. It is intended as a companion to the OHA Privacy Toolkit and you will still need the Toolkit to address any gaps you identify.

This version of the Diagnostic Tool is designed for larger healthcare institutions and not for smaller medical offices.

Instructions

For each question, use the Score Sheet to circle the answer that best describes your current situation. The number corresponding to each answer translates into the following achievement levels:

- 0 – Not adequate (don't know/haven't started)
- 1 – Partially adequate (have made a start, have some key pieces in place)
- 2 – Adequate (have covered the essentials)
- 3 – Best practice (have achieved best practice status)

Some questions may not be applicable for your situation but if you find you are marking off many as “not applicable”, re-examine your thought process as most questions should be applicable under normal circumstances.

Consider adding handwritten notes for each question to explain your answer as this will help you or others to make sense of it when it is reviewed at a later date. This is especially important if you answer "Not Applicable".

Once you have completed the questions, follow the Score Evaluation below the Score Sheet.

Note that an electronic version of the Diagnostic Tool is available on the OHA web site.

Survey Questions

1 – General Privacy Compliance

a) Do you have a written statement?

0 No, we haven't had time to write one

1 Yes, but it’s very basic

2 Yes, we have a written statement that we make available to the public, which describes our information practices (in general terms), provides our contact person's contact information and describes our access, correction, inquiry and complaints procedures

3 Above, plus our written statement describes our other privacy-related procedures

b) Have you developed procedures to support your written statement?

0 No or don't know

1 No, but we generally know what to do based on the written statement

2 Yes, we have developed procedures to ensure that our information practices are followed and to help us deal with requests for access and corrections, as well as privacy-related inquiries and complaints

3 Above, plus we have trained our internal agents (e.g., staff, volunteers and others) to follow our procedures, and we track the effectiveness of these procedures and modify them where necessary

2 – Contact Person

a) Have you designated a contact person to assist you in meeting your privacy obligations?

0 No or don't know

1 No, but staff would know which senior manager to consult

2 Yes, we have a designated a contact person, and we have made his/her contact information available to the public

3 Above, plus we have provided the contact person with the appropriate resources to do the job and we monitor his/her performance

b) What are your contact person's responsibilities?

0 Not sure, we haven't developed a job description

1 Our contact person handles all privacy-related matters

2 Our contact person helps us to comply with the Act, responds to requests for access and corrections, deals with questions and complaints, and ensures our agents are informed of their legal duties under the Act

3 Above, plus our contact person conducts privacy impact assessments, privacy audits and develops privacy-related policies, procedures and tools

3 – Consent

a) What do you do to ensure your patients' implied consent is valid?

0 Nothing in particular or don't know

1 We tell our patients that we need their personal health information in order to provide services to them

2 We give our patients the information they need to understand why we collect their personal health information, how we may use it or disclose it, and what they must do to withhold or withdraw their consent

3 Above, plus we post notices or place brochures about these matters in high traffic areas and waiting rooms

b) What do you do to ensure your patients' express consent is valid?

0 Nothing in particular or don't know

1 We make sure the patient has the capacity to consent or has a substitute decision-maker who has the capacity and authority to consent on the patient's behalf

2 We make sure the patient has the capacity to consent, or has a substitute decision-maker who has the capacity and authority to consent on the patient's behalf, and we ensure that the person giving consent knows why we are collecting the information and how it will be used and/or disclosed

3 Above, plus we also document the consent, whether it was given in writing or orally

4 – Managing Health Information

a) Have you documented the purposes for which you collect your patient's personal health information?

0 No or don't know

1 Purposes are documented but this information is not shared with patients

2 A written statement outlining purposes for collection is available to patients upon request

3 A written statement outlining purposes for collection is posted in a public area

b) Are there policies in place outlining who is authorized to use your patients' personal health information and for which purpose?

0 No or don't know

1 Policies are in place and they include consent requirements

2 Above, plus staff receive training on the use of personal health information

3 Above, plus compliance with the policies are built into agreements with third party agents who use personal health information

c) Is there a policy for disclosing information to family members and friends?

0 No or don't know

1 There is a policy in place but it is not communicated to patients, family members and friends unless the situation warrants it

2 A written policy is posted in a public area and communicated to patients

3 Above, plus staff receive training on the policy

d) Do your volunteers understand their obligations related to protection of privacy?

0 No or don't know

1 We don’t do anything formal, but our volunteers know they need to protect our patients’ privacy

2 All volunteers receive training on privacy

3 Above, plus volunteers are required to sign a non-disclosure agreement

e) Does your organization have an individual who is responsible for disclosure requests from third parties?

0 No or don't know

1 No, but the requester is directed to the supervisor of the clinical area the patient was being treated in

2 Yes, we have an individual with defined responsibilities to address third party requests for disclosure and staff know who to direct requests to

3 Above, plus this individual has the resources and training to address disclosure requests

f) Do you have procedures and policies in place to address a patient request that part of their personal health record not be disclosed to others involved in their care? ("Lock Box")

0 No or don't know

1 We have procedures to flag information a patient wishes not to be disclosed, but we do not have policies in place to respond to a situation where we receive notice that information has been placed in a lock box

2 Yes, we have procedures and policies in place and staff are aware of them

3 Above, plus the patient is informed of our procedures and policies

5 – Accessing Health Records

a) Is there a procedure in place for handling patient requests for access to their personal health information?

0 No or don't know

1 There is a procedure but it is not documented or it is not being followed

2 There is a documented procedure that is easy to locate and used when needed

3 Above plus relevant staff received training on the procedure

b) Are patients informed who to contact if they want to see their personal health record?

0 No or don't know

1 Patients are informed orally if they ask

2 A written statement is available telling patients who to contact and what do if they want to see their personal health record

3 Above plus the written statement is posted in a public area

c) Is there a procedure for patients to complain about a decision to refuse access to a personal health record?

0 No or don't know

1 There is a procedure but it is not communicated to patients

2 Patients receive a written statement outlining the complaint procedure when access is refused

3 Above, plus patients are told that they may contact the Commissioner if they are still not satisfied with the outcome

6 – Correcting Health Records

a) **Is there a procedure in place for handling patient requests for corrections to their personal health information?**

0 No or don't know

1 There is a procedure but it is not documented or it is not being followed

2 There is a documented procedure that is easy to locate and use when needed

3 Above, plus relevant staff received training on the procedure

b) **Once a correction has been made, is there a procedure in place to ensure that anyone who uses the record or to whom the record has been disclosed is informed of the correction?**

0 No or don't know

1 The patient must make a request and provide names and contact information for the people who he/she wants to be informed

2 A notice is provided to anyone who currently uses the record

3 Above, plus a notice is provided to anyone to whom the record has been disclosed

c) **Is there a procedure for patients to include a description of their correction request to be included in their health record if the request was refused?**

0 No or don't know

1 There is a procedure but it is not communicated to patients

2 Patients are told that they can request a written statement outlining the correction request be included in their health record

3 Above plus reasonable efforts are made to disclose the statement to anyone to whom the health record had been disclosed

d) **Do you have a procedure for patients to complain about a refusal to correct a personal health record?**

0 No or don't know

1 There is a procedure but it is not communicated to patients

2 Patients receive a written statement outlining the complaint procedure when a request for correction is refused

3 Above plus patients are told that they may contact the Commissioner if they are still not satisfied with the outcome

7 – Dealing With Health Information

a) **Do you store patient personal health information in a secure manner?**

0 No or don't know

1 Each physician stores his/her patients' own records in the manner that best suits them

2 We have documented standards for storage of personal health information and these standards are communicated to all staff

3 Above, plus we have spot audits to confirm adherence to the storage standards

b) **Do you dispose of patient personal health information in a secure manner?**

0 No or don't know

1 Each physician disposes of his/her patients' own records in the manner that best suits him/her

2 We have documented standards for the disposal of both hard copies and electronic records in a manner that records cannot be recovered in any way

3 Above, plus individuals disposing of records must confirm that they followed hospital procedures when completing the record of disposal and have the resources and training to do their job well

8 – Security, First Steps

a) Does your organization have a security policy?

0 No or don't know

1 We have some documented security practices but no overall policy

2 We have a documented security policy approved by management

3 Above, plus the policy is regularly reviewed and updated when necessary

b) Does your organization have someone with overall responsibility for security?

0 No or don't know

1 No but each senior manager would be responsible for security in their area

2 We have a security officer with defined responsibilities and our staff know who this person is

3 Above, plus our security officer has access to senior management and has the resources and training to do their job well

c) Have you identified all of the personal health information (electronic & hardcopy) that you need to protect?

0 No or don't know

1 We don't have an inventory but we know where most of the information is

2 We have a complete inventory where information is stored and the information is classified as to its handling requirements

3 Above, plus we assign staff members to keep the inventory current and make sure handling requirements are being followed

9 – Security, People

a) Does your organization have security procedures for staff to follow?

0 No or don't know

1 We have documented security procedures in some but not all areas where we need them

2 We have documented procedures for both physical and computer security that line up with our security policy

3 Above, plus each procedure has a designated staff member who regularly reviews and updates it when necessary

b) Do you equip your staff to carry out their security responsibilities?

0 No, don't know or we don't have defined security responsibilities

1 We make security information and tools available but we don't promote them

2 We educate staff on their security responsibilities and provide them with tools such as anti-virus software to be able to meet them

3 Above, plus we have orientation and ongoing awareness training for security and we teach them how to use the tools provided

c) Do your staff understand their security obligations and know what to do if they suspect a security problem?

0 No or don't know

1 We don't formally check but most people know and they know who to call if they suspect a problem

2 All staff and contractors sign a confidentiality agreement and we have a published incident response process

3 Above, plus we reinforce this by requiring that the agreement is signed again annually

d) Do you control access to personal health information on a "Need to Know" basis?

0 No or don't know

1 We give general access only to appropriate staff and trust that they will only use the information they need

2 We limit access as far as possible to what staff need for their jobs and we remove access as soon as it is no longer required

3 Above, plus where we can't strictly limit access we spot-check to ensure no improper use

10 – Security, Institutional

a) Do you have physical security controls in place to protect personal health information?

0 No or don't know

1 The information is locked up or supervised, we have after hours security and our IT facilities are protected

2 Above, plus we have controlled access to the areas with the information at all times (supervision or a badge access system)

3 Above, plus we have a clean-desk policy that is enforced and all staff must wear ID badges and challenge those without them

b) Do you have Information Technology security controls in place to protect electronic personal health information?

0 No or don't know

1 All applications used to access the information require passwords

2 Above, plus we have mandatory standards for passwords and do not allow user IDs to be shared

3 Above, plus we use automation to enforce our password standards

c) Do you have security controls in place to protect the computers used to access personal information?

0 No or don't know

1 Our users must use operating system passwords (for Windows, Mac, Linux etc.) on their computers

2 Above, plus they must use power-on passwords and use locking screen savers when leaving their computers unattended

3 Above, plus we perform spot-checks to make sure our users are following these rules

d) **Do you have security controls in place to protect your computers from viruses**

0 No or don't know

1 We supply anti-virus software to our users and we have a mechanism to communicate urgent security issues to our staff

2 Above plus we automate updates to the software and have an incident management process to respond to attacks which is known to all staff

3 Above plus we have a process to make sure long-term solutions for problems are implemented where appropriate

e) **If you provide staff with remote network access to your systems, do you provide a secure way for them to do so?**

0 No or don't know

1 We provide a virtual private network, or equivalent, for remote staff access

2 Above, plus we only allow access from computers with our standard software image that includes a personal firewall

3 Above, plus we have mechanisms to make sure that our computers are running the correct software

f) **Do you protect personal health information that you transport outside of your office environment?**

0 No or don't know

1 We use reputable companies to transport the information

2 Above, plus we use locked boxes or equivalent for hard copy information

3 Above, plus we use tamper-evident packaging and check that the right quantities arrive at the destination

g) Do you protect personal health information on computers being repaired, sold or disposed of?

0 No or don't know

1 We only use reputable companies for servicing, purchasing or disposing of our computers

2 Above, plus we ensure personal health information is properly erased before these computers are released

3 Above, plus we design our systems so that the minimum amount of personal health information is stored on personal computers

11 – Security, Sustaining Security

a) Do you make sure that all affiliates and third party providers meet your security requirements?

0 No or don't know

1 We don't check on this but we only deal with those who have good reputations and no past history of problems

2 We make sure all our contracts spell out the security requirements we expect them to meet

3 Above, plus we provide them with any information that may help them comply and we periodically check that they are complying

b) Do you have a plan to be able to restore critical personal health information if the primary copies are not available?

0 No or don't know

1 We make backup copies of all critical personal health information and test that the copies are usable

2 Above, plus we have tested disaster and business recovery plans that will restore this information in crisis situations

3 Above, plus we regularly re-test our disaster and business recovery plans to make sure they still work effectively

c) Do you have controls to make sure that changes to your IT environment don't introduce new security problems?

0 No or don't know

1 We have separate development/test/production IT environments and our developers/testers cannot change the production environment

2 Above, plus we have a formal change control process which looks at the security implications of any proposed changes

3 Above, plus we have security checks built into our IT development and procurement processes and we use a Threat Risk Assessment process

d) Do you regularly check that you are in compliance with your security policy?

0 No, don't know or we don't have a security policy

1 We don't have a formal review program but we do security spot checks

2 We collect all necessary audit information, conduct regular reviews by independent staff and track issues found until they are resolved

3 Above, plus we also have external assessments/audits and review the results with senior management

12 – Research

a) When and how do you collect personal health information for research purposes without consent?

0 Not sure or don't know

1 We have a written policy on the collection of personal health information for research purposes, but it's very basic

2 Our procedures require us to comply with the Act's requirements concerning research plans and research ethics board approval, and we only collect personal health information from those parties who are permitted by law to give us such information

3 Above, plus we enter into written agreements concerning the protection of the information with health information custodians who give us the information

b) When and how do you use personal health information for research purposes without consent?

0 Not sure or don't know

1 We have a written policy on the use of personal health information for research purposes, but it's very basic

2 Our procedures require us to use personal health information for research purposes without consent only if the law permits us to do so, and only if conducted under a research plan that a research ethics board has approved (or we follow the rules for research approved outside Ontario if the personal health information originates outside of Ontario)

3 Above, plus we have developed procedures to safeguard the information

c) When and to whom do you disclose personal health information for research purposes without consent?

0 Not sure or don't know

1 We have a written policy on the disclosure of personal health information for research purposes, but it's very basic

2 Our procedures require us to disclose personal health information to researchers without consent only if we enter into a written agreement with the researcher to protect the information and we receive from the researcher a written application, a written research plan, and a copy of a research ethics boards' approval of the research plan

3 Above, plus our procedures require us to impose additional obligations on the researcher in certain circumstances

13 – Fundraising

a) **Do you ensure that you have your patients' implied consent before using their names and mailing addresses for fundraising purposes?**

0 No or don't know

1 Not sure, but someone usually tells our patients that our foundation will contact them for fundraising purposes

2 Yes, we tell patients that we will use and disclose their names and mailing address for fundraising purposes and we tell them how they can opt-out of receiving fundraising solicitations

3 Above, plus we tell patients how to opt-out of receiving fundraising solicitations in our notices, signs and brochures, as well as in every fundraising solicitation

b) **Have your fundraisers been properly trained on privacy matters?**

0 No, fundraisers are not given any particular rules or guidelines to follow

1 Yes, fundraisers are asked to be respectful of patients' privacy, and we give them limited guidance

2 Yes, we inform our fundraisers on privacy compliance – for example, we tell them not to solicit donations from a patient for at least 60 days' and we tell them not to communicate a patient's state of health or health care when they contact the patient for fundraising purposes

3 Above, plus we audit our fundraiser's practices from time to time to ensure compliance

14 – Managing Contracts & Agents

a) **Have you taken steps to protect the personal health information that you provide to your external agents?**

0 No or don't know

1 Yes, we only use reputable companies who have privacy policies but we don't have any written policies on this

2 Yes, we investigate potential agents for their privacy compliance before hiring them and we include privacy protection clauses in our contracts with our agents

3 Above, plus we monitor our contracts regularly and when necessary, we enforce them

15 – Oversight

a) What should you do if a privacy breach occurs?

0 Not sure or don't know

1 Our contact person would deal with any breach on an ad hoc basis

2 Our procedures require us to contain the breach and to notify anyone affected by it

3 Above, plus we review whether our policies and procedures adequately protect personal health information

b) How do you contain a privacy breach?

0 Not sure or don't know

1 Our contact person would direct us

2 Our procedures require us to retrieve any personal health information that has been disclosed, ensure that the person who was not authorized to receive the information did not make or keep copies of the information, and get that person's contact information in case there's a need to follow-up

3 Above, plus we determine whether the breach allows unauthorized access to any other personal health information and, if so, take all appropriate steps to stop further breaches

c) What do you tell the individual(s) whose personal health information was disclosed without authorization?

0 Not sure

1 We would apologize and take responsibility for the disclosure

2 Our procedures require us to explain what and how much personal health information was affected, explain immediate and long-term steps we and others have taken to rectify the breach, and make note of the unauthorized uses/disclosures in (or linked to) the affected personal health records

3 Above, plus we designate one person who would communicate with the public about the breach

Score Sheet and Analysis

Please go through each of the Survey Questions and circle the number that best corresponds to the level of compliance that you have achieved to date.

Note: you may wish to make photocopies of this Score Sheet so that you can repeat the survey at a future date or complete separate surveys for different areas of your institution's operations.

Questions	Answers (circle one per question)			
General Privacy Compliance				
1.a)	0	1	2	3
1.b)	0	1	2	3
Contact Person				
2.a)	0	1	2	3
2.b)	0	1	2	3
Consent				
3.a)	0	1	2	3
3.b)	0	1	2	3
Managing Health Information				
4.a)	0	1	2	3
4.b)	0	1	2	3
4.c)	0	1	2	3
4.d)	0	1	2	3
4.e)	0	1	2	3
4.f)	0	1	2	3
Accessing Health Records				
5.a)	0	1	2	3
5.b)	0	1	2	3
5.c)	0	1	2	3
Correcting Health Records				
6.a)	0	1	2	3
6.b)	0	1	2	3
6.c)	0	1	2	3
6.d)	0	1	2	3
Dealing With Health Information				
7.a)	0	1	2	3
7.b)	0	1	2	3

Questions	Answers (circle one per question)			
Security, First Steps				
8.a)	0	1	2	3
8.b)	0	1	2	3
8.c)	0	1	2	3
Security, People				
9.a)	0	1	2	3
9.b)	0	1	2	3
9.c)	0	1	2	3
9.d)	0	1	2	3
Security, Institutional Safeguards				
10.a)	0	1	2	3
10.b)	0	1	2	3
10.c)	0	1	2	3
10.d)	0	1	2	3
10.e)	0	1	2	3
10.f)	0	1	2	3
10.g)	0	1	2	3
Security, Sustaining Security				
11.a)	0	1	2	3
11.b)	0	1	2	3
11.c)	0	1	2	3
11.d)	0	1	2	3
Research				
12.a)	0	1	2	3
12.b)	0	1	2	3
12.c)	0	1	2	3
Fundraising				
13.a)	0	1	2	3
13.b)	0	1	2	3
Managing Contracts & Agents				
14.a)	0	1	2	3
Oversight				
15.a)	0	1	2	3
15.b)	0	1	2	3
15.c)	0	1	2	3

Score Evaluation

If you have a 0 or 1 in any of the above answers, you should review that particular section of the Privacy Toolkit and take additional steps to achieve compliance with the Act.

If you have a 2 in any of the above answers, you have achieved compliance with the Act. You might consider reviewing that particular section of the Privacy Toolkit and take additional steps to achieve best practices.

If you have a 3 in any of the above answers, you have achieved compliance with the Act and have also implemented the proposed best practices. Well done! Keep in mind that you are responsible for on-going training, maintenance and monitoring of your privacy program.

Index

Index

Index

Index

Index