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

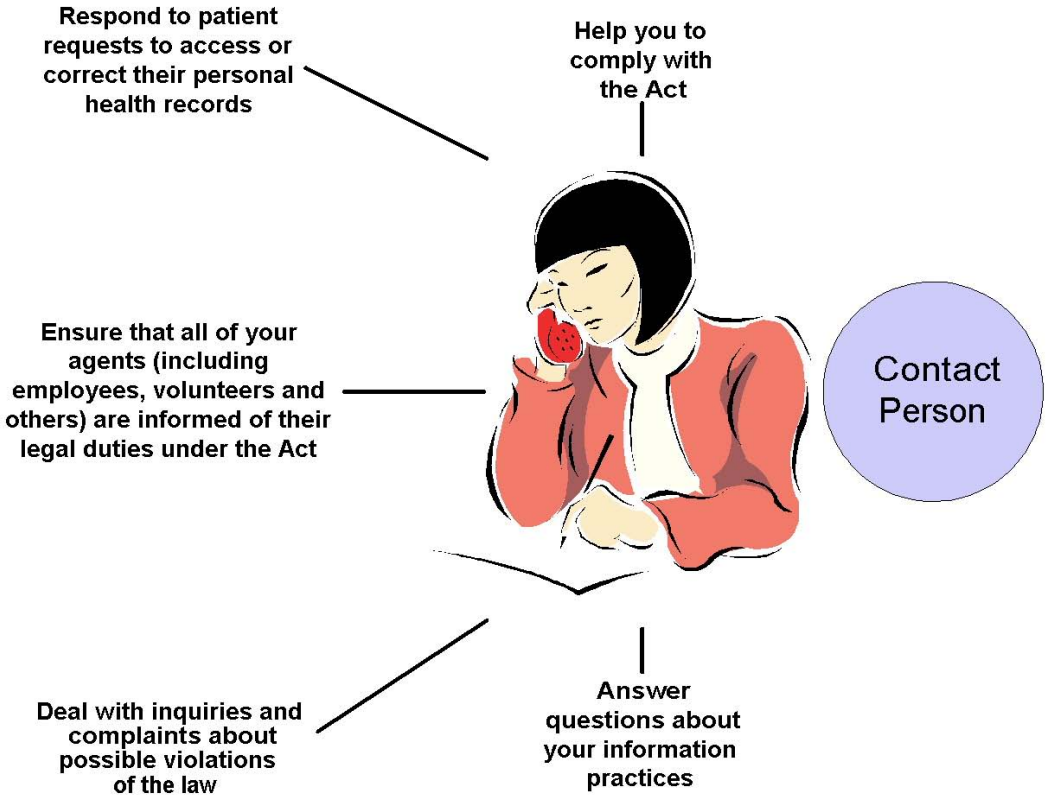
Key Points

- 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

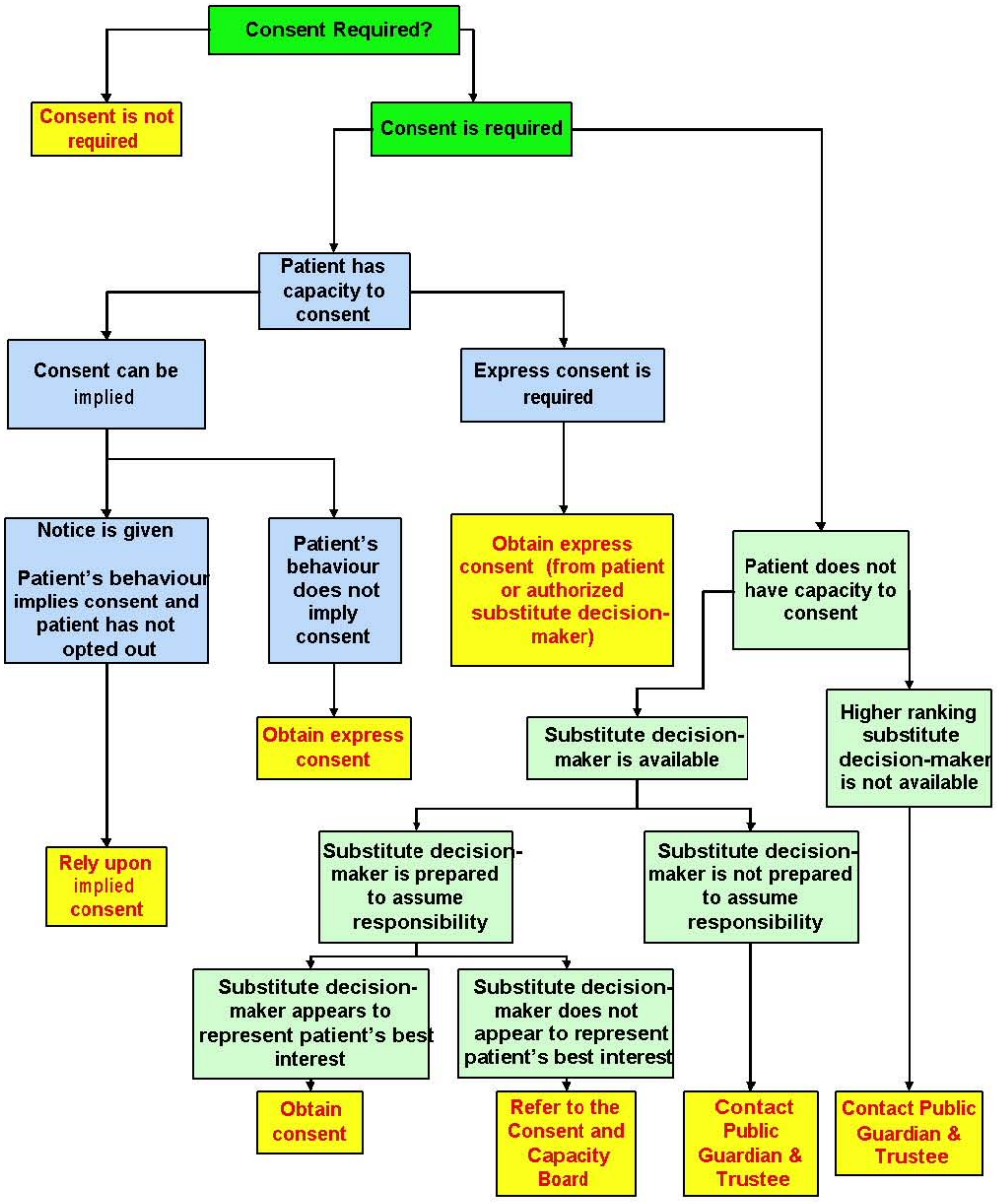
3, 5, 6, 9, 16(2), 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 32, 33, 36, 37, 38, 39, 42, 43, 44, 45, 46, 47

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

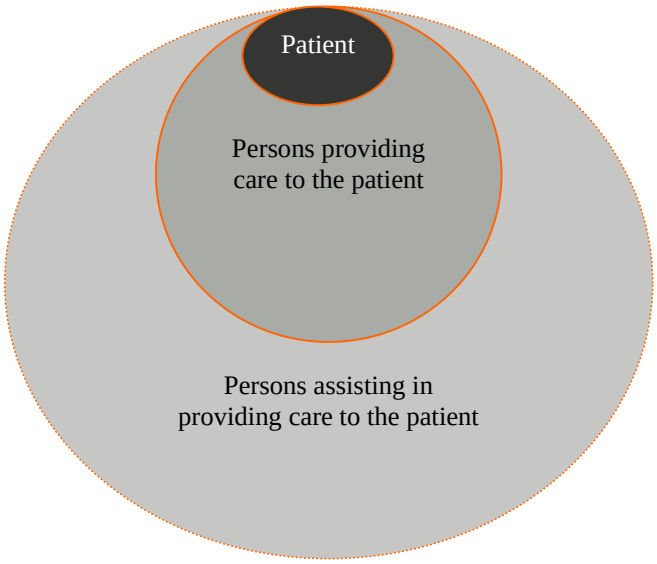
- Develop policies on who is authorized to use your patients' personal health information and for which purpose.
- Inform health care professionals and staff about:
  - the purposes for which they may use personal health information,
  - the consent requirements for use,
  - when other information will 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 Services 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, Childrens' 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

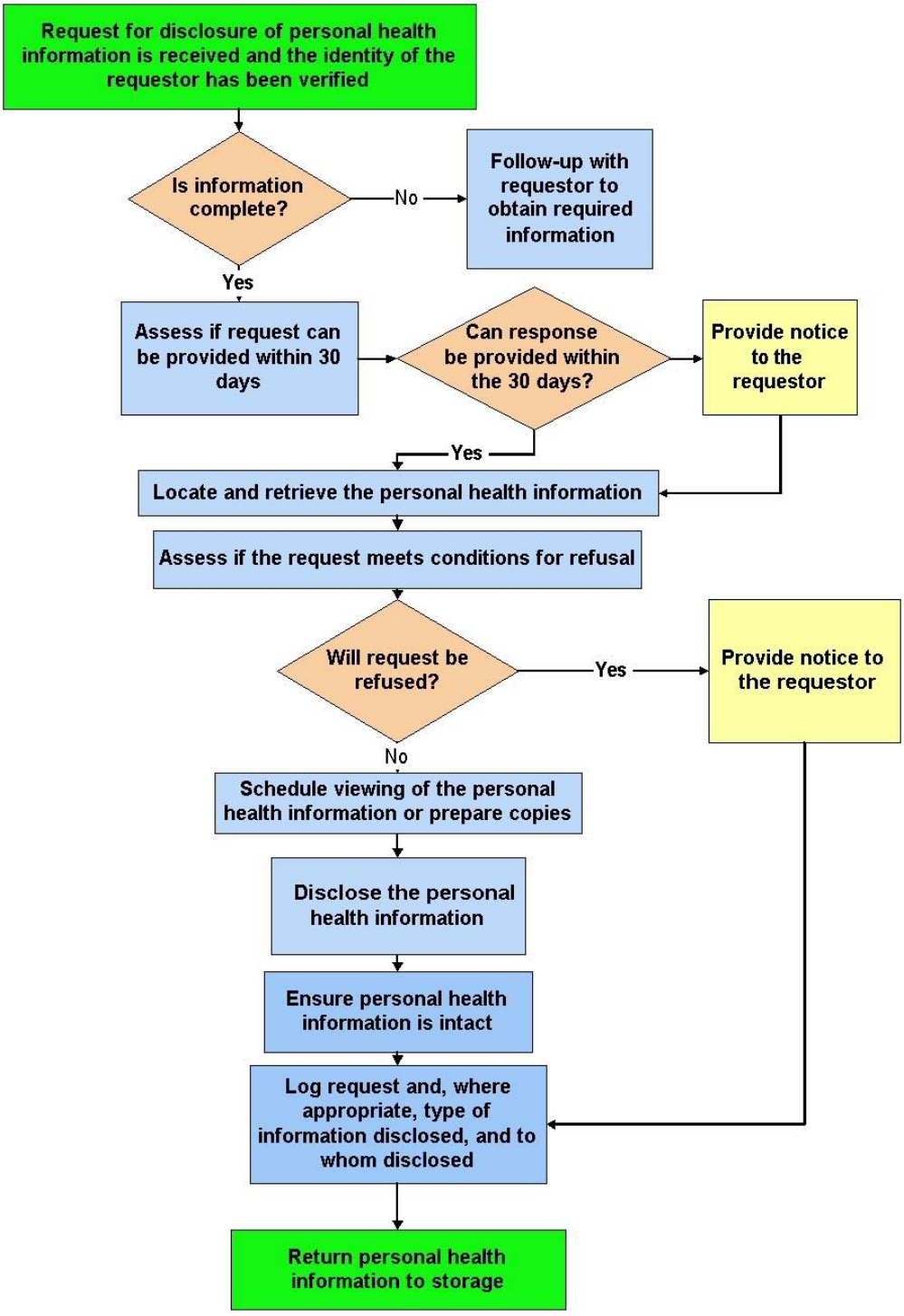
Related Sections of the Act

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.

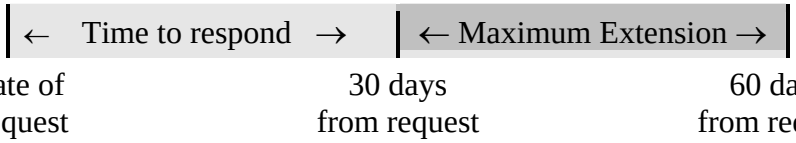
The fee you charge cannot exceed either a prescribed amount or, if no amount is prescribed, a reasonable cost recovery charge.

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

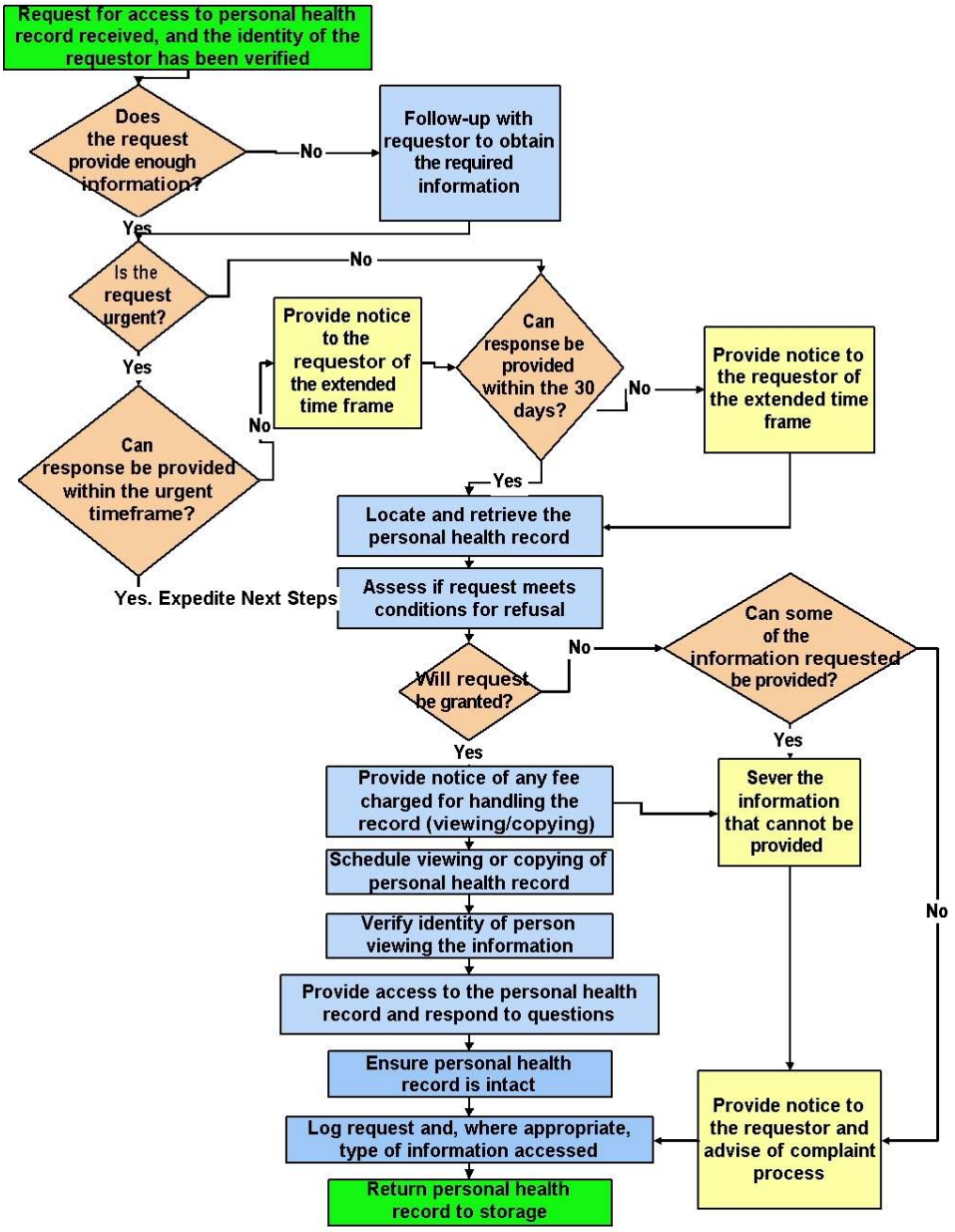
51, 52, 53, 54, 72 (1)(d)

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

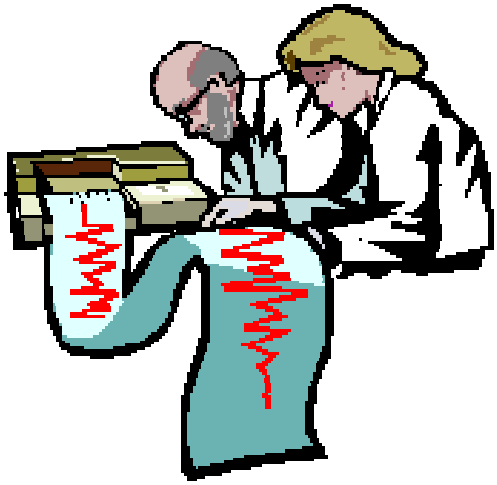


Table of Contents

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

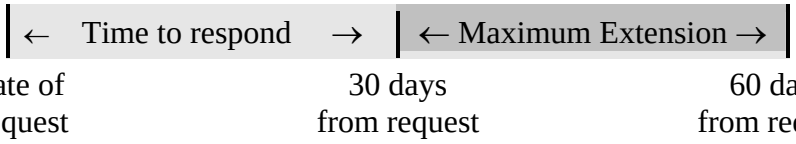
You do not have to correct a record:

- 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

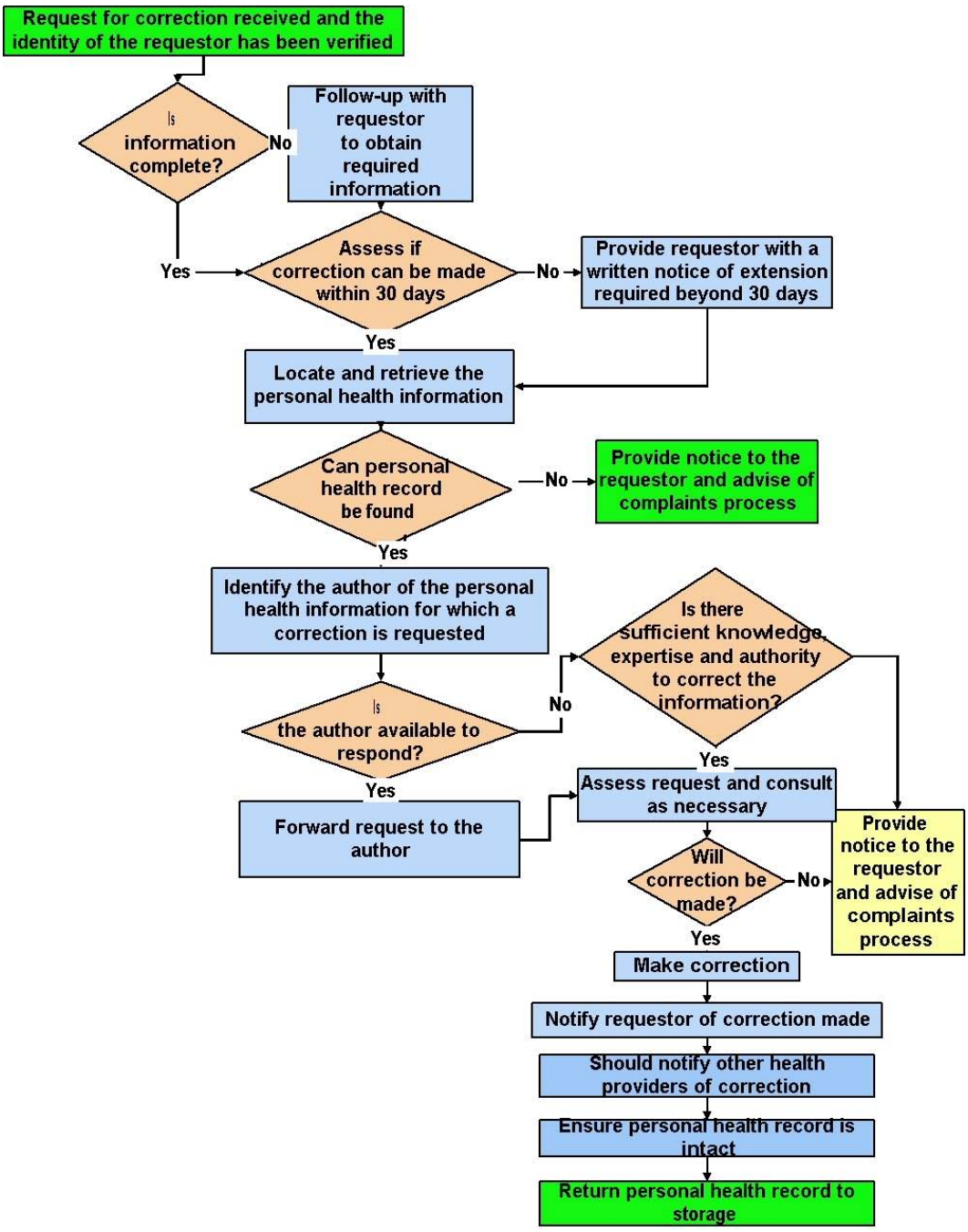
55

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 _____