

Government of the Northwest Territories
Department of Health and Social Services



Health Information Act Guide

*A Practical Guide to the Northwest Territories'
Health Privacy Legislation*

Health Information Act Guide

This document is a general guide to the *Health Information Act*. It is designed to help readers understand the key provisions of the Act.

The topics covered in this guide are of necessity limited; it does not provide legal advice. The Department of Health and Social Services urges readers who require specific advice on legal matters to seek legal counsel.

If any inconsistency exists between this guide and the *Health Information Act*, the Act takes precedence.

Note: The content of this guide, including templates and other resource materials, is available to any reader and can be used for the purpose of ensuring compliance with the *Health Information Act*. When using the materials, readers are advised to appropriately credit the Government of the Northwest Territories, which holds the copyright for the guide.

Health Privacy
Policy, Legislation and Communications
Department of Health and Social Services
Government of the Northwest Territories
P.O. Box 1320, Yellowknife, NT X1A 2L9

To download a copy of the *Health Information Act Guide*, or other related information, visit the Department of Health and Social Services website:

www.hss.gov.nt.ca/health/slides/health-privacy-protecting-your-health-information



July 2015

Contents

Contents	iv	Chapter 2. Custodians and Agents.....	19
Introduction to the		Introduction	19
<i>Health Information Act Guide</i>	1	Custodians' Roles, Duties, and Responsibilities	20
Introduction	1	Agents' Roles, Duties, and Responsibilities.....	22
The <i>Health Information Act Guide</i>	2	Designated Contact Persons' Roles, Duties, and Responsibilities.....	24
How to use the <i>Health Information Act Guide</i>	3	Resources	25
Resources	4	Test Your Knowledge	26
Chapter 1. Scope of the Act	5	Summary of Key Concepts	27
Introduction	5	Chapter 3. Consent.....	29
Purpose of the <i>Health Information Act</i>	6	Introduction.....	29
Basic Principles of the <i>Health Information Act</i>	6	Patients and Substitute Decision-Makers.....	30
Definitions.....	6	Knowledgeable Consent	31
Who the Act Applies to.....	9	Elements of a Valid Consent.....	31
What the Act Applies to.....	10	Implied Consent.....	32
When the Act Applies – Hierarchies of Privacy Rules	13	Express Consent.....	33
Resources	15	Consent Conditions and Express Instructions ..	35
Test Your Knowledge	16	Withdrawal of Consent.....	36
Summary of Key Concepts.....	17	Resources	37
		Test Your Knowledge	38
		Summary of Key Concepts	39

Chapter 4. Collection	41	Keeping a Record of Disclosures	66
Introduction	41	Resources	67
Basic Privacy Principles	42	Test Your Knowledge	68
When You Can Collect Information	42	Summary of Key Concepts	69
Collecting Information from Third Parties	42		
Required Notice	43	Chapter 7. Disclosure for Research and	
Patient Identifiers.....	43	Research Ethics Committee	71
Collection with Recording Device.....	44	Introduction	71
Resources	45	Research Ethics Committee	72
Test Your Knowledge	46	Research Ethics Committee	
Summary of Key Concepts	47	Review and Approval	72
		Research Agreement Requirements	73
Chapter 5. Use	49	Patients' Express Consent.....	74
Introduction.....	49	Research Fees.....	75
Basic Privacy Principles	50	Disclosure Requirements –	
When You Can Use		General Requirements.....	75
Personal Health Information	50	Resources	76
Authorized (Secondary) Uses of Health		Test Your Knowledge	77
Information Allowed by the HIA	50	Summary of Key Concepts.....	78
De-Identifying Health Information.....	51		
Data Matching.....	52	Chapter 8. Information Managers	
Additional Uses of Health Information		and Information Management Agreements	79
by Public Custodians	52	Introduction.....	79
Resources	53	What is an Information Manager?.....	80
Test Your Knowledge	54	Information Management Agreement	
Summary of Key Concepts.....	55	Requirements.....	80
		Resources	82
Chapter 6. Disclosure	57	Test Your Knowledge	83
Introduction.....	57	Summary of Key Concepts.....	84
Basic Privacy Principles	58		
When You Can Disclose.....	58		
Discretionary Disclosures.....	58		
Mandatory Disclosures	64		
Authenticating the Recipient.....	65		

Chapter 9. Information and Privacy Commissioner 85

Introduction.....	85
IPC Appointment and Role	86
IPC Powers and Duties	86
Annual Report.....	87
Procedure and Evidence on Review	87
Resources	88
Test Your Knowledge	89
Summary of Key Concepts.....	90

Chapter 10. Access to and Correction of Personal Health Information 91

Introduction.....	91
Patients' Right to Access Their Own Records....	92
Exceptions to the Right of Access.....	93
Access Request Process.....	94
Patients' Right to Have Their Information Corrected	101
Correction Request Process.....	101
Resources	106
Test your Knowledge	107
Summary of Key Concepts.....	108

Chapter 11. Privacy Breach 109

Introduction.....	109
What Is a Privacy Breach?	110
Privacy Breach Prevention.....	110
Privacy Breach Response	112
Privacy Breach Complaints and Review Process	114
Resources	117
Test Your Knowledge	118
Summary of Key Concepts.....	119

Chapter 12. Offences and Limitation of Liability..... 121

Introduction.....	121
Offence and Penalties.....	122
Limitation of Liability	122
Resources	123
Test Your Knowledge	124
Summary of Key Concepts.....	125

Resources 127

Introduction – Resources..... 127

Orientation Checklist for Employees.....	128
How to Read an Act.....	129

Chapter 1. Scope of the Act – Resources..... 130

Does the HIA Apply? – Infographic	131
---	-----

Chapter 2. Custodians and Agents – Resources..... 132

Custodian Responsibility Checklist	133
Sample Oath of Confidentiality	136

Chapter 3. Consent – Resources 137

Notification of Collection of Personal Health Information	138
---	-----

Chapter 4. Collection – Resources 139

Sample Consent to be Photographed/Recorded.....	140
---	-----

Chapter 5. Use – Resources 141

Use of Personal Health Information at-a-Glance	142
--	-----

Chapter 6. Disclosure – Resources..... 144

Disclosure of Personal Health Information at-a-Glance	145
---	-----

Disclosure Decision Trees – Disclosure with Express Consent.....	148
--	-----

Disclosure Decision Trees – Disclosure without Express Consent.....	149
---	-----

Chapter 7. Disclosure for Research and Research Ethics Committee – Resources.....	150	Chapter 7. Disclosure for Research and Research Ethics Committee	176
Processing Research Requests at-a-Glance	151	Chapter 8. Information Managers and Information Management Agreements	177
Chapter 8. Information Managers and Information Management Agreements – Resources.....	152	Chapter 9. Information and Privacy Commissioner	177
Comparison of Information Management Agreements, Information Sharing Agreements, and Research Agreements	153	Chapter 10. Access to and Correction of Personal Health Information.....	178
Chapter 9. Information and Privacy Commissioner – Resources	154	Chapter 11. Privacy Breaches	179
Chapter 10. Access to and Correction of Personal Health Information – Resources	155	Chapter 12. Offences and Limitation of Liability	180
Formal Access Request: Suggested Tasks and Timelines	156	Links to the Act.....	181
Access Request Timelines.....	162	Part 1. How the Act Applies	181
Correction Request Timelines	163	Part 2. Roles and Responsibilities.....	181
Access Requests at-a-Glance	164	Part 3. Consent and Substitute Decision Makers.....	182
<i>Health Information Act: Access to Personal Health Information Process.....</i>	<i>166</i>	Part 4. Collection, Use, Disclosure and Protection of Personal Health Information	183
<i>Health Information Act: Correction to Personal Health Information Process.....</i>	<i>167</i>	Part 5. Access to and Correction of Personal Health Information.....	186
<i>Health Information Act: Appeal and Review Process.....</i>	<i>168</i>	Part 6. Review and Appeal	187
Chapter 11. Privacy Breach – Resources	169	Part 7. Information and Privacy Commissioner	190
Chapter 12. Offences and Limitation of Liability– Resources	170	Part 8. General	191
Answer Key	171	Index	193
Chapter 1. Scope of the Act	171		
Chapter 2. Custodians and Agents.....	172		
Chapter 3. Consent	172		
Chapter 4. Collection.....	173		
Chapter 5. Use	174		
Chapter 6. Disclosure	175		

Introduction

to the *Health Information Act Guide*

Introduction

The Northwest Territories' *Health Information Act* (HIA) was passed in March 2014. It protects people's privacy by governing the collection, use, sharing, and storage of their personal health information. The Act recognizes both individuals' rights to access their own information and the needs of health service providers to collect, use, and share patient information in order to provide best care. Penalties may be imposed if the rules of the Act are not followed.

The *Health Information Act Guide* (HIA Guide) explains the rights of patients and the responsibilities of health service providers, set out under the HIA. The HIA Guide is intended to be the main HIA resource for frontline health service providers and persons working to support the delivery of health services, including administrative staff, management, records management personnel, and other support roles.

The HIA Guide will help you understand how to protect the privacy of people who visit your clinic, health centre, hospital, or pharmacy. It explains the HIA and how it affects your work. When you are at work, you may overhear conversations between patients and health service providers. You might be directly involved in managing medical records and other confidential information. Privacy and trust are particularly important where health information is concerned. People who have concerns about their privacy may not want to share their personal health information, which could make it difficult to provide them with the best care possible.

The goal of the HIA Guide is to promote a patient-focused, balanced approach to the collection, use and sharing of personal health information that supports the delivery of best care, where patients trust their health service providers and participate in how their information is managed.

The Health Information Act Guide

The HIA Guide explains the HIA and its Regulations. Health service providers and their employees, contractors, and volunteers will use it as a guide in their daily work. At the end of each chapter, you will find the following sections:

Resources

- Lists of additional information such as forms and templates related to the topic discussed in the chapter. They are available at the end of the HIA Guide. Click on the hyperlink or use the bookmarks to view them.
- Information related to the topic that is available from other sources.

Test Your Knowledge

- A short case study or quiz you can use to make sure you understand the information in the chapter. The answers are found in the HIA Guide. Click on the hyperlink or use the bookmarks to view them.

Summary of Key Concepts

- An overview of essential information you can print out to use as a quick reference.

At the end of the HIA Guide, you will find the following:

Additional Resources

- Sample forms, posters, and templates you can customize to use in your organization. You can access these forms by using the hyperlink in the Resources section in each chapter or going directly to this section of the HIA Guide.
- Tools that can be used to apply the HIA to a specific task. For example:
 - A valid consent checklist identifies key requirements for consent.
 - Decision tree diagrams will help you to process requests for the release of information.

Answer Keys

- Answers and explanations related to the case studies and quizzes in Test Your Knowledge.

Links to the Act

- Section numbers of the Act cross-referenced to the chapters in the HIA Guide. If you want more information about a section of the HIA, refer to the Links to the Act.

Updates

- New information about HIA legislation and procedures. Look for them at the [DHSS website health-privacy-protecting-your-health-information](http://www.hss.gov.nt.ca/health/slides/health-privacy-protecting-your-health-information)
- Updates should be printed out and inserted in this guide.

If you have questions about the information in the HIA Guide or suggestions to improve it, please contact us using the website link.

How to use the *Health Information Act Guide*

1. **Start by reviewing the contents page of each chapter in the HIA Guide.**

The structure of the HIA Guide follows the steps used to collect, use, and share personal health information.

2. **Read through each chapter.**

Pay particular attention to the information that is most relevant to your work.

3. **Refer to the Resources at the end of each chapter.**

This section includes scenarios, templates, and forms to assist you in your day-to-day work. It will help you become familiar with the HIA.

4. **Complete the Test Your Knowledge section.**

This section includes case studies and quizzes to help you become familiar with the content of the HIA. Your supervisor may ask you to submit your completed quiz to demonstrate that you have met learning objectives.

5. **Refer to the Summary of Key Concepts for quick reviews.**

6. **Use this guide as an easy reference in your daily work.**





If you work for a health organization or health service provider, your supervisor will give you a checklist of sections you need to complete as part of your orientation. It will be important for you to read and understand some sections right away. You will refer to other sections occasionally as you continue learning how to do your job.

If you are an employer, providing consistent training about the HIA is a key responsibility under the HIA. It makes good business sense to provide training in a way that is easily understood by your health service providers and staff. You may use the HIA Guide as part of your orientation program. See the Resources section at the end of the HIA Guide for a link to a sample checklist you can use to identify the sections that new employees should review.

Related Information

Icons

Throughout this guide, you will see small black and white icons that provide a quick reference to other resources. The icons used are shown below.

Images	Where to find them
 Reference Page	Reference to a section in the HIA Guide
 Light bulb	Key concepts
 Information	Resources in the HIA Guide, Privacy Risk Toolkit, or other sources
 Tool Box	Reference to the Privacy Risk Toolkit

Resources

These resources and templates are available at the end of the Health Information Act Guide. Click on the hyperlink or use the bookmarks to view them.

Orientation Checklist for Employees

You may use the HIA Guide as part of your orientation program. See the Resources section at the end of the HIA Guide for a link to a sample form you can use to identify the sections that new employees should review as part of their orientation.

How to Read an Act

Use this quick-tip guide to learn how to find information in an Act and properly reference sections of an Act.

The following additional resources also are available from DHSS website [health-privacy-protecting-your-health-information](#):

- Privacy Risk Toolkit
- Tutorials
- Training Sessions
- *Health Information Act*
- *Health Information Regulations*
- Privacy policies

1 Scope of the Act

Introduction

Everyone who works in the health care system needs to be aware of the laws regulating the collection and use of people's personal health information. These laws are set out in the *Health Information Act* (HIA) and the *Health Information Regulations*.

Chapter 1 begins by defining the terms used in the HIA and the Regulations. It then identifies the organizations and individuals who must follow the Act and explains when the HIA must be applied. A question-and-answer flow sheet will help you decide whether the HIA applies to a specific situation. The difference between identifying and non-identifying information is explained. Examples of both types of information are given.

The chapter concludes by discussing how the HIA is related to other GNWT privacy legislation. It explains which laws take precedence in specific situations, that is, the hierarchies of privacy rules.

This chapter includes the following **key concepts**:

1. Purpose of the HIA
2. Basic principles of the HIA
3. Definitions of terms used in the HIA
4. Who the HIA applies to
5. What the HIA applies to
6. When the HIA applies
7. Hierarchies of privacy rules

Purpose of the *Health Information Act*

The HIA has two main purposes:

- Make rules about the collection, use, disclosure, and security of personal health information that protect the privacy of the people the information is about.
- Facilitate the provision of health services.

(See HIA s.2, *Purpose of the HIA*.)

Basic Principles of the *Health Information Act*

Privacy Principles

- Only information that is necessary for the purpose for which it is collected, should be collected.
- Collect, use and share de-identified information unless identifiable information is necessary.
- Collect, use and share as little information as necessary.
- Patients must be told how their personal health information will be used, who will have access to their information, and how it will be protected.
- Patients' personal health information must not be collected, used or shared unless it is required to provide a health service or for another purpose authorized by either the patient or by law.

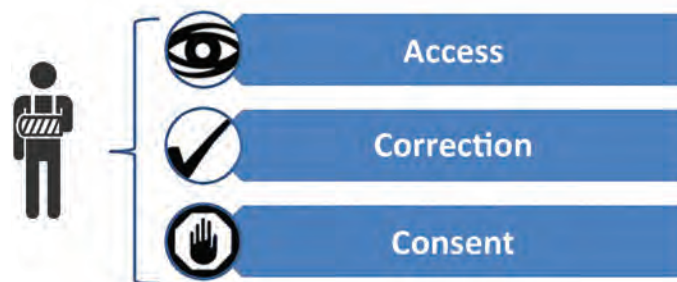
Figure 1: Privacy Principles for Custodians and Agents



Patients' Rights

- Patients have the right to see their personal health information.
- Patients can ask to have personal health information corrected.
- Patients can authorize other people to access their personal health information.
- Patients have the right to set limits on the collection, use, and sharing of their personal health information.
- Patients have the right to know what happens to their personal health information.

Figure 2: Patients' Rights



Definitions

Part 1 of the HIA defines terms used in the legislation. The following list interprets many of the key terms to help you understand the HIA and its companion document, the *Health Information Regulations*. Refer to the HIA and the Regulations for additional details when necessary.



Information about these terms is also provided in other sections of the HIA Guide. Search in the [Index](#) for relevant page numbers.

access request A patient's (or substitute decision-maker's) request to see the patient's medical record. The Regulations set out fees for patients' access requests. HSSAs, DHSS and private custodians designate contact persons to respond to all access requests.

agent Employees, volunteers, appointees, contractors, and information managers acting on behalf of a custodian. Physicians and pharmacists employed or contracted by DHSS, an HSSA, or another private custodian are agents and not custodians.

collect To acquire, gather, obtain, or receive information.

contact person A person designated to respond to questions and complaints from the public. This can be the health information custodian or someone designated by the custodian.

correction request A patient's request that information in her or his medical record be changed.

custodian See *health information custodian*.

disclose To share information in any way – verbally, electronically, or in printed material.

extra-territorial research ethics committee Research ethics committee outside of the Northwest Territories that is recognized by legislation that is equivalent to the HIA in another Canadian province or territory.

health information custodians Health information custodians specifically named by the HIA. They include:

- Department of Health and Social Services (DHSS)
- Health and Social Services Authorities (HSSAs)
- private physicians
- private pharmacists

health service An observation, examination, assessment, or procedure in relation to an individual, or the care of an individual, that is carried out, provided, or undertaken for one of the following health-related purposes:

- protection, promotion, or maintenance of health
- prevention of conditions adverse to health
- testing or examination of a body part or substance
- diagnosis
- treatment
- rehabilitation (such as physiotherapy)
- health care for the ill, injured, disabled, or dying
- addiction services, including addiction treatment, counselling, and detoxification¹
- mental health counselling²
- organ and tissue donation and transplantation²
- an ambulance service
- a service provided by a pharmacist or under the direction or supervision of a pharmacist

The term “health service” includes both insured and non-insured services and both physical and mental health services.

health service provider A person or organization that provides a health service. This includes providers in other jurisdictions, such as Alberta.

individual A person, whether living or deceased.

Information and Privacy Commissioner (IPC) The person who provides privacy oversight for the HIA. The IPC for the *Access to Information and Protection of Privacy Act* (ATIPPA) is automatically the IPC for the HIA as well.

¹ Regulation 2

² Regulation 2

information manager A person or organization that provides information technology (IT), information management (IM), and information systems (IS) services for a custodian or manages, stores, or transforms personal health information on behalf of a custodian. An information manager may provide transcription services, technical support, remote back-up, and off-site records management and retrieval. More than one organization may enter information in an electronic health information system. The Technology Services Centre (TSC) and the Yellowknife Health and Social Services Authority are information managers. The IT support for a private physician's clinic or private pharmacy is an information manager.

personal health information Identifiable health information about a patient, as in the following examples:

- information about the individual's medical history and health services provided
- name and contact information collected when an individual visits a health care provider
- information used to determine if someone qualifies for an Extended Health Benefit (EHB), an escort during medical travel, or other health service or benefit
- eligibility or registration for a health service or benefit
- a personal health number, other identifying number, symbol, or other identification assigned to an individual in respect of health services or health information
- prescription information
- information about an individual's donation of a body part or bodily substance
- information about payment for a health service for an individual

privacy impact assessment (PIA) a written document created by a health information custodian to assess the potential impacts on and risks to the privacy of personal health information stored in or associated with a communication technology or information system.

public custodian DHSS or HSSA.

record Information in any form that is made and stored in any manner, such as an audiovisual recording, book, drawing, electronic record, email, handwritten or electronic note, patient chart, photograph, prescription, video, written record, or x-ray or other diagnostic image. The term "record" does not refer to a computer program, electronic health information system, or any other mechanism that creates or stores the record.

research A scientific study or systematic investigation conducted to discover new information or new applications of existing information, or to test or evaluate the results of existing research.

Research does not mean a use of information for a purpose referred to in sections 35(a–e) or (g–j) or section 37 of the HIA. Analysis done by custodians for internal and health system planning and management is not considered research. Studies carried out as part of the regular scope of work of the custodian are not considered research; however, studies completed by a custodian for personal and academic purposes are considered research.

research ethics committee A research ethics committee (REC) designated under the HIA. This could be an existing ethics committee designated by the Minister through an order, or a new committee set up through the Regulations. The Aurora College Research Ethics Committee is designated an REC under the HIA.

researcher A person or organization, including a health information custodian, that collects or uses (or wants to collect or use) personal health information for research purposes.

substitute decision-maker A person referred to in paragraphs 25(1)(c) to (i) of the HIA who acts on behalf of an individual, specifically in respect of an individual's rights regarding personal health information, and not in respect of treatment.

use To handle or apply information for a purpose, including to reproduce or transform it. In the context of the HIA, "use" does not mean to collect or share information.

Who the Act Applies to

The HIA applies to health information custodians and their agents when they collect, use, disclose, retain, or destroy personal health information in the course of providing health services.

Custodians include:

- Department of Health and Social Services (DHSS)
- Health and Social Services Authorities (HSSAs)
- physicians who are not employed by the DHSS or HSSAs (“private physicians”)
- pharmacists who are not employed by the DHSS or HSSAs (“private pharmacists”)

Public Custodians

Public custodians are the DHSS and the HSSAs. When a custodian is an organization named in the HIA, the administrative head of the organization assumes the responsibilities of a custodian. The Deputy Minister of the DHSS is ultimately responsible for the DHSS. The Chief Executive Officer of each HSSA is ultimately responsible for that HSSA.

(See HIA s.7, Custodians: persons responsible; Health Information Regulations s.1(1)(2).)

Private Custodians

A private custodian is any health information custodian who is not a public custodian. Private and public custodians have the same roles, duties, and responsibilities.

Example

The Department of Health and Social Services and the Health and Social Services Authorities are **public custodians**.

Physicians and pharmacists in private practice are **private custodians**.

Agents

If you work for a health information custodian, you are considered an agent under the HIA. Agents include salaried employees, contractors, appointees, information managers, volunteers, summer students, and anyone else working for a custodian. Agents can be physicians, pharmacists, nurses, clinic assistants, pharmacy technicians, other members of the medical staff, clerk interpreters, administrative staff, records management staff, and office managers.



(See [Chapter 8, Information Managers and Information Management Agreements](#))

Examples

Mary is a clinic assistant at a health centre. She collects information from patients in order to schedule appointments and create patient records. Mary is an **agent**. The HSSA is a **custodian**.

Matthew is a physician working as a locum for an HSSA. Matthew is an **agent** of the **custodian**, the HSSA. Matthew must follow the standards, policies, and procedures of the custodian. He must also meet the standards of practice of his regulated health profession.

Thomas is a physiotherapist working for an HSSA. Thomas is an **agent** of the **custodian**, the HSSA. Thomas must follow the standards, policies, and procedures of the custodian. He must also meet the standards of practice of his regulated health profession.

The roles and responsibilities of custodians and agents are discussed in Chapter 2.

What the Act Applies to

The HIA applies to personal health information in the custody or under the control of custodians as it relates to physical and mental health services. Since mental illness and addiction can be inter-related, the HIA applies to addiction services as well.

The HIA applies only to health information in the custody or under the control of custodians and agents. The Act does not set out rules relative to health information in the hands of others, with the exception of researchers.

The HIA does not apply to social services such as the Healthy Family program and family violence services.

Personal Health Information

Personal health information is health information about a patient that identifies the individual. If you are not sure if something is considered to be personal health information under the HIA, it may help to first determine whether the information is

collected, used, or shared as part of a health service defined in the HIA.

Examples of personal health information include:

- medical records
- health care plan registration and renewal information
- medical travel approval, booking, and payment information
- Extended Health Benefits (EHB) and Non-Insured Health Benefits (NIHB) eligibility, approval, and payment information
- pharmacists' records of patients' third-party medical insurance information
- mental health and addictions counselling records
- patient-specific public health and health promotion records, such as participation in a stop-smoking program

The table below lists common personal health information that is kept in patients' medical records.

Table 1. Personal Health Information in Medical Records

Registration Information	Diagnostic, Treatment, and Care Information	Scheduling / Billing Information
Client names Address Phone numbers Sex Date of birth Personal health number Contact name Contact relationship Contact address Contact phone number Alerts Chart number	Family and social history Past medical history Immunization history Medication Allergies Lab orders and results Progress notes Consults Diagnostic imaging reports Prescriptions Alerts	Appointment date Appointment time Reason for visit Payer Amount owing Units Hospital admit date Medical travel approval, booking, and payment information

Note: Information about health services providers, health service facilities, or their identifiers (for example, facility code, practitioner license number) is not currently included as personal health information under the HIA.

Note: The HIA definition of personal health information differs from the definition of personal information in the *Access to Information and Protection of Privacy Act* (ATIPP) and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Note: The HIA allows health information custodians to collect, use, or share non-identifying information. Non-identifying means the information cannot be used to discover the name of any specific person. Anonymous statistical information is non-identifying (see the example below).



Be careful – with computers and search engines, only a few facts can be enough to identify a person.

Example

Mary is reporting on attendance at an immunization clinic. She says, “Eighteen people got the flu vaccine today.” This is **non-identifying information**.

Mary does not say, “Eighteen people got the flu today – Bob, Mary, Paul, Emma, my aunt Jessie,...” The names of people who were immunized are not necessary for the daily report, so only the numbers are given. The fact that each person was given a flu shot is noted in his or her personal health record.

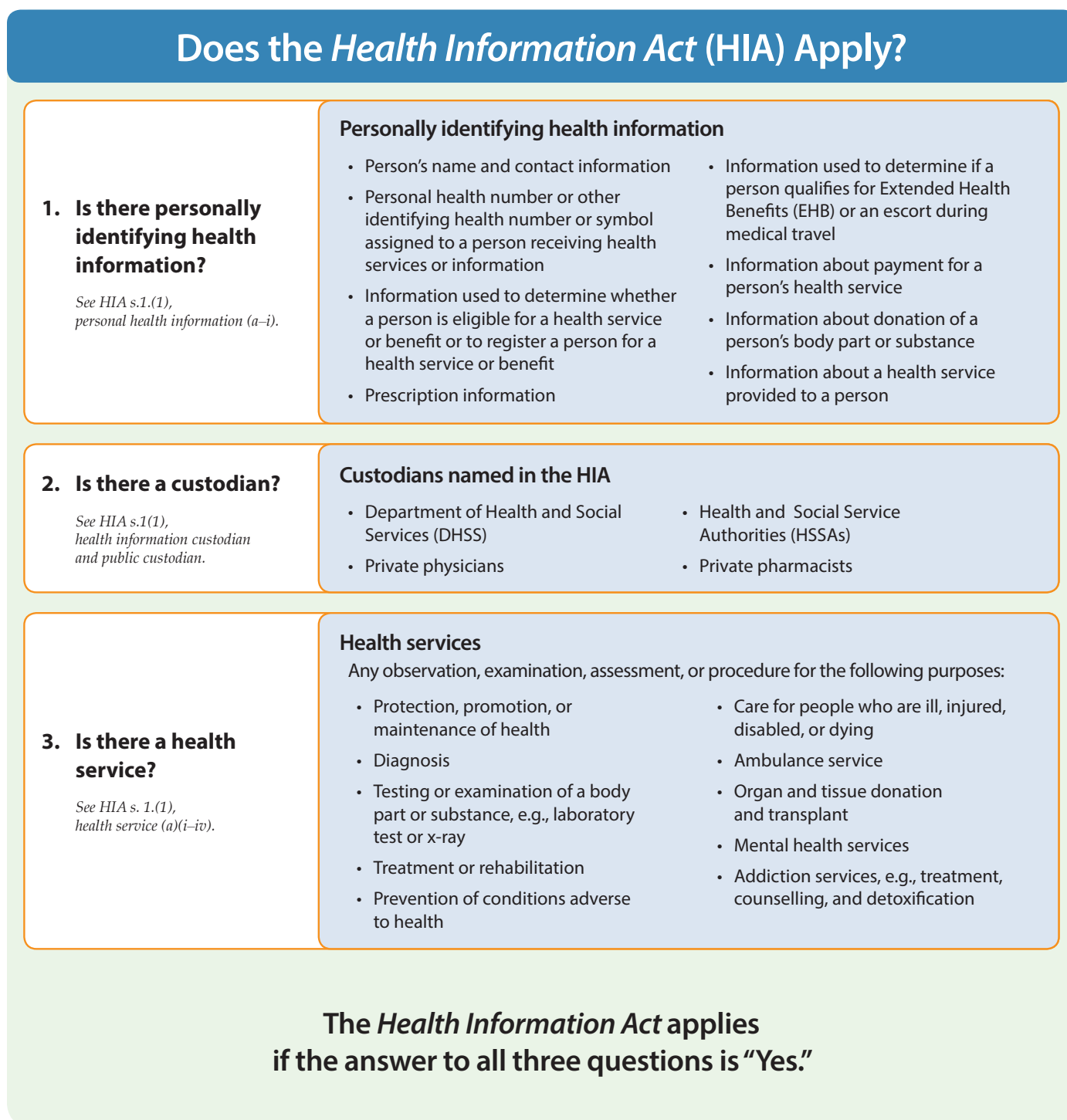
Exceptions

The HIA rules apply to the collection, use, and sharing of all personal health information and medical records kept by a custodian, except:

- records related to the health of a child or parents that are kept as part of official records governed by the *Child and Family Services Act*
- adoption records
- professional licensing records and records of complaints about licensed health professionals
- human resources and employee records, such as staff immunization records or duty to accommodate records created for other business reasons (i.e., records that are not collected to provide health services)

Use the following table to determine whether the HIA applies in a particular situation.

Figure 3. Does the HIA Apply?



When the Act Applies – Hierarchies of Privacy Rules

Which legislation and rules do you need to follow? Remember, it is possible that more than one privacy law applies to records created by an organization.

Privacy legislation differs depending on where you work; the type of organization, agency, or industry in which you work; and the type of personal information you collect, use, and share. Custodians and business owners are responsible for knowing the legislation that applies to them. Existing legislation has been changed to prevent conflicts with the HIA. If the services you provide fall under other legislation, review it to make sure your policies and procedures are up-to-date. Many health professions and associations have also developed standards of practice and codes of ethics. If you belong to one of these groups, it is your responsibility to know and follow these guidelines.

When personal health information is concerned, the HIA overrides all other NWT Acts **unless** another Act, or a provision of it, takes priority over the HIA.

The HIA does not:

- override a requirement to share personal health information during a lawsuit or other legal action
- prevent a court from requiring a witness to testify
- override the *Evidence Act*
- override the *Electronic Transactions Act*, which allows notices required in writing to be sent electronically
- stop the handling and destruction of records required by another NWT law or in accordance with GNWT records schedules (unless future regulations under the HIA specifically prevent these actions)
- prevent the handling and destruction of records that is required by a federal law, for example, the *Food and Drugs Act*

(See HIA s.4, *Scope of the Act*; s.5, *Conflicts*; s. 6, *Application*)

Public Custodians

The HIA prevails over ATIPP, however it does not limit a person's right to obtain information under ATIPP. ATIPP, passed in 1996, focuses on public government records. It does not refer in detail to health information and does not apply to private physicians and private pharmacists. Public records such as contracts and government correspondence remain governed by ATIPP. If a government record contains personal health information, access to that record may still be granted under ATIPP if the personal health information it contains can be hidden (blacked out or "severed").

(See HIA s.4, *Scope of the Act*; s.5, *Conflict or inconsistency*.)

When someone makes a request for access to records governed by both the HIA and ATIPP, the person processing the request follows the HIA rules for the record that includes personal health information covered by the HIA and the ATIPP rules for the government record.

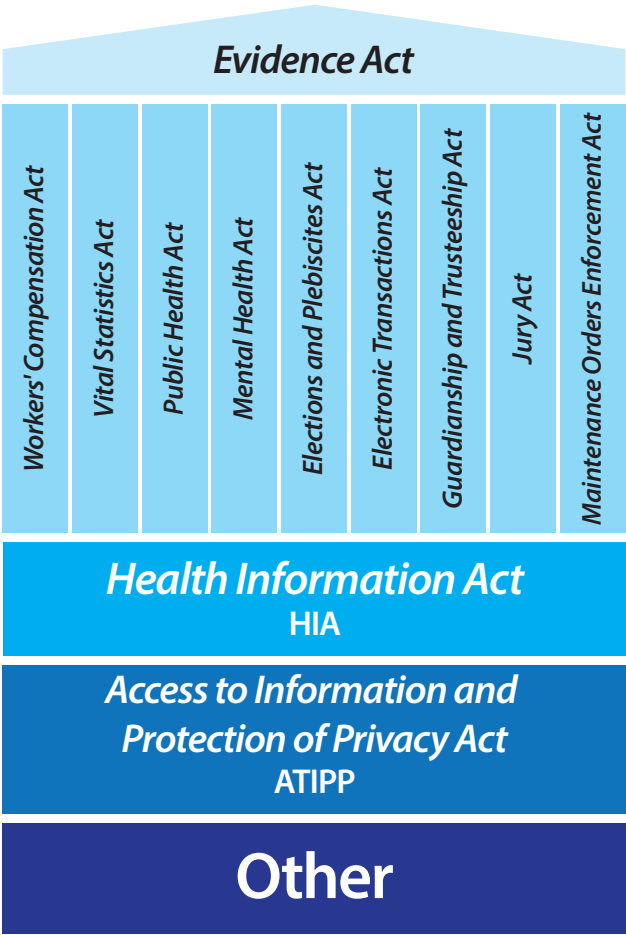
Example

Martha makes an access request to see a list of who has accessed her medical record at her health centre. As part of the same request, she asks to see the policies and procedures her health centre has to limit who has access to patient records. HIA applies to part one of her request. ATIPP applies to part two.

(See HIA s.6(2), *Access request and ATIPP*.)

Public custodians must follow the below hierarchy when it comes to complying with the law:

Figure 4. Hierarchy of Privacy Rules – Public Custodians



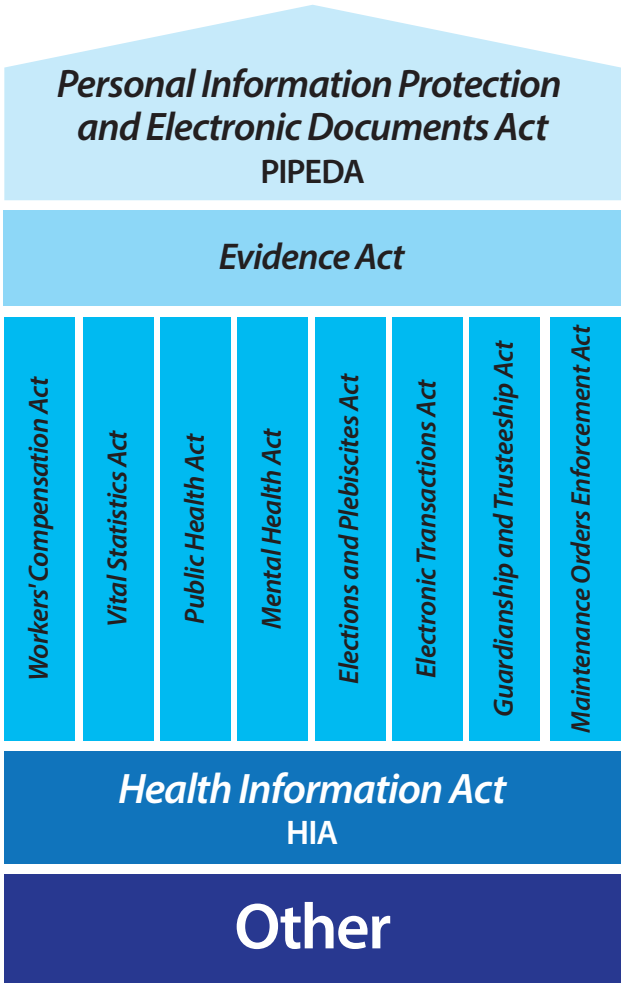
Private Custodians

Private physicians and private pharmacists must follow *Personal Information Protection and Electronic Documents Act* (PIPEDA) legislation. This may change if the Federal Government grants PIPEDA substantial similarity status to the HIA. At this time, private pharmacists and physicians will follow both PIPEDA and the HIA.

If substantial similarity status is granted, then private pharmacists and physicians will follow just the HIA. This would reduce the regulatory burden for private pharmacists and physicians. This will let all custodians designated under the HIA follow the same privacy framework.

Private custodians must follow the below hierarchy when it comes to complying with the law:

Figure 5. Hierarchy of Privacy Rules – Private Custodians



(See HIA s.4, *Scope of the Act*; s.5, *Conflicts*; s. 6, *Application*; s.198 – s.207, *Consequential amendments*.)

Resources

The following resource is available at the end of the Health Information Act Guide. Click on the hyperlink or use the bookmarks to view.

Does the HIA Apply? – Infographic

Use the infographic to help you to determine whether the HIA applies to a particular patient and situation.

The following publication is available online:

Gerber, Ben. (2010). *OECD Privacy Principles*. Retrieved from <http://oecdprivacy.org/>

Chapter 1. Scope of the Act – Test Your Knowledge

The following quiz applies to many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 171](#).

1. Which of the following are examples of personal health information as defined by the HIA?
 - a. name, date of birth, and address of patient receiving health services
 - b. progress note on a patient at an outpatient clinic
 - c. laboratory requisition for a patient
 - d. receipt for crutches purchased at a store
 - e. physician's business card from the health centre
 - f. pharmacy dispensary patient record
 - g. medical travel approval, booking, and payment information
2. What are the purposes of the HIA?
 - a. to prevent patients from seeing their medical records
 - b. to protect patients' personal health information
 - c. to make it difficult to share patient information
 - d. to set rules that custodians must follow when they collect, use, and share patients' personal health information
3. Who must follow the HIA?
 - a. Department of Health and Social Services
 - b. physicians who own and operate a private medical clinic
 - c. a store that sells first-aid supplies
 - d. tobacco cessation programs managed by the DHSS or the HSSAs
 - e. a medical clinic at an industrial site that is managed by a physician

Chapter 1. Scope of the Act – Summary of Key Concepts

1. **Purposes** of the HIA

- To make rules about the collection, use, disclosure, and security of personal health information that protect the privacy of the people the information is about
- To facilitate the provision of health services

2. **Custodians and agents** must follow the HIA.

3. The HIA applies when:

- There is **personally identifying health information**.
- The information is in the care of a **custodian**.
- This information was originally collected to deliver a **health service**.

4. HIA privacy rules pertain only to **health services**.

5. **Hierarchies** of privacy rules

- For public custodians (the DHSS and the HSSAs)
 - The *Evidence Act* overrides the HIA.
 - The HIA overrides the ATIPP and all other NWT Acts, with the exceptions below.
 - Certain provisions of other acts override the HIA. (*See HIA s.198.*)
- For private custodians (private physicians and private pharmacists)
 - The PIPEDA overrides the HIA. This may change if the similarity status of PIPEDA is granted.
 - The *Evidence Act* overrides the HIA.
 - The HIA overrides all other NWT Acts.
 - Certain provisions of other acts override the HIA. (*See HIA s.198.*)

2 Custodians and Agents

Introduction

Custodians and agents collect, use, store, and share personal health information in order to provide health services. The *Health Information Act* (HIA) states what custodians and agents must do to keep patients' information private and secure. It is important for you to understand your own responsibilities and those of the people you work with. You should also be aware of the responsibilities of other people who are involved in caring for patients.

This chapter includes the following **key concepts**:

1. Responsibilities of a custodian under the HIA
2. Responsibilities of an agent under the HIA
3. Responsibilities of a designated contact person under the HIA

Custodians' Roles, Duties, and Responsibilities

Custodians must comply with the HIA and its Regulations. They must establish policies and procedures and implement safeguards to protect patients' personal health information. They also are responsible for training agents and making sure patients are notified about how their health information will be collected, used, and shared.

1. Policies, Standards, and Procedures

Custodians must develop or adopt standards, policies, and procedures to comply with the HIA and its Regulations.

(See HIA s.8, Standards, policies, and procedures required.)

Custodians also must:

- Share the custodian's policies and procedures with the DHSS if requested
- Keep records to document that policies and procedures are being followed
- Review and update policies and procedures regularly, at least annually

(See Health Information Regulations s.13(3))

2. Safeguards

Custodians must protect the confidentiality of personal health information and the privacy of patients. This includes personal health information that is stored, used or shared outside the NWT by custodians or their agents. Custodians must develop and maintain reasonable safeguards to respond to any threat to the security, confidentiality and integrity of personal health information in their custody or under their control. Custodians must maintain administrative, technical, and physical safeguards to protect against unauthorized access, use, disclosure, alteration, destruction, or disposal of patient records, loss of patient records, and theft.

(See HIA s.85, Measures for protection of information.)

Custodians should assess current practices to make sure they comply with HIA requirements. Measures to maintain safeguards must be proportionate to any threat to the security, confidentiality and integrity of personal health information.

To do this, custodians should:

- Conduct an annual review to document current practices, evaluate the effectiveness of current safeguard measures, and ensure compliance with the HIA
- Identify any gaps and prepare an implementation plan
- Implement appropriate controls to protect personal health information

(See Health Information Regs s.13(2).)



(See [Chapter 11, Privacy Breach.](#))

In order to comply with the HIA, safeguards developed and implemented by custodians must specifically include:

- measures to protect personal health information through an assessment of re-identification risk and the application of de-identification procedures as required
- measures to protect network infrastructure from interruption and unauthorized access and use
- the use of authentication and encryption to protect personal health information stored electronically
- measures to prevent and respond to problems involving hardware and software that might threaten the security, confidentiality, or integrity of personal health information
- measures to protect hardware and software from unauthorized access and use
- measures to protect personal health information stored and transported on removable media

- a requirement that personal health information be maintained in a designated area subject to appropriate security safeguards
- a requirement that access to personal health information be monitored on an ongoing basis for the purpose of ensuring that only authorized access is occurring
- procedures that provide for the recording, reporting and investigation of security and privacy breaches
- procedures that provide for effective prevention of, response to and remediation of security and privacy breaches

(See *Health Information Regulations s.13(1)(a)-(j)*.)

- procedures to recognize privacy or security breaches, contain and mitigate them, notify the individual(s) affected, the Information and Privacy Commissioner and other parties as necessary, and review and respond to breaches

(See *HIA s. 87, Duty to give notice; Health Information Regulations s.14-15*.)

3. Additional Requirements

Custodians must ensure that personal health information is accurate and complete when collecting the information and before using and sharing it, and must ensure access to records with the use of organized records management systems. Safeguards and good organizational and professional practices will assist custodians in ensuring that personal health information is accurate and complete when they collect it and before they use and disclose it.

(See *HIA s.88, Accuracy of information*.)

Each custodian must name at least one agent as its HIA designated contact person.

(See *HIA s.12, Designated contact person*.)

Custodians must conduct a privacy impact assessment (PIA) whenever a new or updated information system or communication technology is being considered for the collection, use, or disclosure of personal health information. The PIA must be shared with the Information and Privacy Commissioner.

(See *HIA s.89(3), Privacy impact assessment to IPC*.)

A custodian who is involved in research must meet the requirements of the HIA and the Regulations, in particular the requirement to get research ethics committee approval.

(See *HIA s.8, Standards, policies and procedures required; s.85–89 Protection of personal health information; Health Information Regulations s.8, s.13*.)



(See [Chapter 7, Disclosure for Research and Research Ethics Committee](#))

When collecting information from patients, custodians and agents must inform patients how their information may be used or shared and that the custodian and agent will follow the requirements of the HIA to properly protect their personal health information. Custodians and agents must inform patients through a posted notice or be able to explain this directly to the patient. Only if patients receive this notice can custodians and agents assume patients have given implied consent to having their information collected, used, and shared. Notices about how patients' health information may be collected, used, or shared can include posters, pamphlets, and short videos. These should be placed where patients will see or hear them.

(See *HIA s.15(2), Notice: purposes of collection, use or disclosure*.)

Custodians and agents also should help patients decide how their personal information can be used. They have a responsibility to assist patients prepare access applications. This is called a “duty to assist.”

Example

Alfred has been offered a job. His potential employer asks Alfred to provide his medical record to prove that he is fit for work. When he visits his community health nurse in the health centre, Alfred asks the nurse to give the employer his medical record.

The nurse reviews Alfred's medical record with him. She suggests that only a few key sections of the medical record be sent to the employer.

Alfred was very happy to get the nurse's advice. He didn't know that a lot of the information in his medical record didn't affect his ability to work and didn't have to be sent to the employer.

The nurse had a “duty to assist” Alfred to make good choices about how his personal health information would be shared.

When patients make access requests, health information custodians must make every reasonable effort to respond accurately and quickly. Develop and maintain procedures for tracking and responding to access requests. Ensure proper timeframes are followed in responding to access requests.



(See [Chapter 3, Consent](#), and [Chapter 10, Access and Correction](#).)

4. Training

Custodians should train and monitor all agents to make sure they follow HIA standards, policies, and procedures in place to support compliance with the HIA. To do this, custodians can provide:

- on-the-job orientation
- privacy awareness overview training
- access to policies and procedures
- mentoring
- supervision
- compliance reviews



Your privacy and security training awareness program should provide the same basic information for everyone in the organization. Agents in some positions

will require additional training. Each privacy awareness training program should include regular updates and reminders. The Privacy Risk Toolkit suggests ways to develop a privacy awareness training program in your practice.



(See [Resources – Custodian Responsibility Checklist](#).)



(See the [Privacy Risk Toolkit](#))

Agents' Roles, Duties, and Responsibilities

Agents may have direct access to personal health information or be directly involved in providing health services. They also may see or overhear patients or their health information. It is important for them to be familiar with privacy legislation.

Agents may have many administrative responsibilities:

- providing health services to patients
- checking patients in when they arrive at a health centre

- processing access requests
- registering NWT residents for health care coverage
- determining Extended Health Benefit (EHB) program eligibility and coverage
- arranging medical travel
- receiving prescriptions from patients
- dispensing medications
- using personal health information as part of managing a practice or health system

Example

Ayla is a new patient at the health centre. The clinic assistant starts a new patient record for Ayla and asks Ayla for her health care card, name, date of birth, address, and phone number. The clinic assistant confirms that the information that Ayla gives the clinic assistant matches the information in the system.

The HSSA is a **custodian** as defined by the HIA. The clinic assistant is an employee of the HSSA and is defined by the HIA as an **agent**. The Act allows the clinic assistant to collect, use, and share personal health information to provide health services. The clerk accesses Ayla's insurance information to make sure that the information in the patient record is accurate. For example, the clerk makes sure Ayla's health care insurance number is valid and her address is correct.

Agents cannot collect, use, share, manage, retain, or dispose personal health information unless they are allowed to do this by the HIA and the custodian. These actions must be part of their regular duties or work assigned to them. Agents must use personal health information only for the purposes the custodian is allowed to use it for. They cannot use the information for any other purpose.

(See HIA s.9, Agents; s.10, Compliance with Act and regulations.)

Examples

Mary is a clerk at a health centre. She collects information from patients in order to schedule their appointments and update their medical records. Mary cannot use a patient's information in order to contact him about a community event.

Emily is a clinic assistant at a primary care clinic. She has access to health care registration information. Emily cannot use the information to create a list of colleagues' birth dates in order to plan parties.

Agents must follow standards, policies, procedures, and safeguard measures developed by the custodian to implement and comply with the HIA. Custodians can monitor employees' work to make sure the standards, policies, procedures, and safeguards are being followed.

Examples

The HSSA has an Electronic Medical Record (EMR) system that creates electronic patient records. Each authorized user of this software system has her or his own user account. Whenever an agent uses the EMR to access a patient's record, the agent is identified in an audit log. The custodian monitors agents' use of the EMR to make sure they are following the rules that protect patients' health information.

(See HIA s.11, Compliance required: standards, policies and procedures.)

Designated Contact Persons' Roles, Duties, and Responsibilities

A custodian must name at least one agent as the designated contact person. The contact person is someone in the organization, clinic, or health centre who understands the HIA and its regulations. This person must also be familiar with the custodian's privacy policies and procedures.

The contact person has the following responsibilities:

- Promote staff compliance with the HIA:
 - Identify privacy compliance issues for the custodian.
 - Recommend when a privacy impact assessment is required.
 - Participate with the custodian in an annual review to make sure current administrative, physical, and technical safeguards protect the privacy of patient records.
 - Assist in developing and maintaining privacy, security, and operational policies and procedures.
 - Make sure agents are aware of their responsibilities and duties under the HIA.
 - Interpret the HIA for agents and patients.
 - Respond to internal questions about processing access and correction requests.
 - Assist in ensuring the overall security and protection of health information held by the custodian.
- Respond to questions and complaints from the public about the collection of information and information practices.
- Process and respond to access and correction requests.
- Receive complaints about non-compliance with the HIA.
- Act for the custodian in dealings with third parties and the Information and Privacy Commissioner.

A nurse-in-charge, clinic manager, quality risk manager, records coordinator, or other agent may be designated as the contact person. A large health care organization may have a full-time contact person, co-contact persons, or assistant contact persons. Physicians or pharmacists in the private sector may be their own HIA contact persons or may name others as contact persons.

Example

Pauline has been working at an HSSA for many years. She is a manager in the Health Records Department. One of her jobs is to manage requests for access to patient health information. She is also one of the HSSA's ATIPP Coordinators. Under the HIA, she will be the **designated contact person** for the hospital.

Remember, contact persons are agents and may act only on behalf of custodians. They must keep the custodians informed of their actions. A contact person may be authorized to make routine decisions without discussing them with the custodian. In other cases, the contact person makes recommendations to the custodian and must not act without the custodian's authorization.

(See HIA s.12, *Designated contact person*.)

Resources

The following resources and templates are available at the end of the Health Information Act Guide. Click on the hyperlink or use the bookmarks to view them.

Custodian Responsibility Checklist

Custodians under the Act must ensure their agents follow the standards, policies, and procedures outlined in the HIA. Use this quick-tip guide to learn how to assess your current practices and identify areas in which they could be improved.

Sample Oath of Confidentiality

An Oath of Confidentiality for agents and custodians could be based on this template. Custodians may modify and develop your own document. This sample form includes a statement that the person will respect privacy, has received training and can ask questions his or her supervisor.

These resources are available from DHSS website [health-privacy-protecting-your-health-information](http://www.hss.gov.nt.ca/health/slides/health-privacy-protecting-your-health-information) (<http://www.hss.gov.nt.ca/health/slides/health-privacy-protecting-your-health-information>).

Privacy Risk Toolkit

Roles and Responsibilities of Designated Contact Persons – Video

Chapter 2. Custodians and Agents – Test Your Knowledge

The following case study applies many of the key concepts in this section. Read the example and answer the questions below. Then check your answers with the answer key on [page 172](#).

Example

Mary and her supervisor, Pauline, work for a Health and Social Services Authority.

Mary was hired as a health clerk who will register patients for appointments with the community health nurse.

When Mary was hired, she attended HIA Privacy Awareness Overview training. She also read policies and procedures specific to her new job. At a meeting with her supervisor, Mary asked questions in order to understand her job better. She signed an oath of confidentiality in which she promised to keep patients' health information safe. She indicated that she received training and knows she can ask her supervisor when she has additional questions.

Pauline is the authority on the HIA at her HSSA. She provides health information privacy training to Mary and the other agents. She expects her employees to follow the HIA, and she monitors their work. Pauline is responsible for the confidentiality of all patient health information under her control.

1. Who is the custodian?
2. Who is the agent?
3. Who is the designated contact person?
4. Is personal health information collected at the HSSA?
5. Who does the custodian designate to deliver training and monitor compliance?

Chapter 2. Custodians and Agents – Summary of Key Concepts

1. Responsibilities of a **custodian** under the *Health Information Act*
 - Develop or adopt standards, policies, and procedures to comply with the HIA.
 - Use administrative, technical, and physical safeguards to protect health information.
 - Tell patients how their personal health information may be collected, used, and shared.
 - Help patients access their personal health information (“duty to assist”).
 - Do privacy impact assessments for new and updated information systems and communication technologies.
 - Train and monitor all agents to make sure they follow the HIA.
 - Name at least one agent as the HIA designated contact person.
2. Responsibilities of an **agent** under the HIA
 - Use personal health information only for the purposes specified by the HIA.
 - Follow the custodian’s policies and procedures to implement the HIA.
3. Responsibilities of a **designated contact person** under the HIA
 - Act only on behalf of the custodian.
 - Keep the custodian informed of actions.
 - Make routine decisions without discussing them with the custodian, or make recommendations to the custodian.
 - Promote staff compliance with the HIA.
 - Respond to questions and complaints from the public about the collection of information and information practices.
 - Process and respond to access and correction requests.

3 Consent

Introduction

Under the *Health Information Act* (HIA), custodians and agents cannot collect, use, or share patients' personal health information without their consent except where allowed or required by the HIA or another act. Patients have the right to set limits on how much information is shared, and with whom. Patients should never be surprised by anything that happens to their information. They should be aware that consent related to personal health information is not the same as consent for treatment.

This chapter includes the following **key concepts**:

1. Patients and substitute decision-makers
2. Knowledgeable consent
3. Elements of a valid consent
4. Implied consent
5. Express consent
6. Consent conditions and express instructions
7. Withdrawal of consent

Patients and Substitute Decision-Makers

The following people can make decisions about their own personal health information:

- any patient 19 years and older
- any patient under 19 who is a mature minor

The following people are substitute decision-makers for people who cannot act on their own behalf:

- a patient's guardian or parent if the patient is under 19 and is not a mature minor
- a patient's guardian, trustee, or legal representative
- a person who holds the patient's power of attorney or the person named in a personal directive
- anyone authorized in writing by a patient who is mentally competent
- a deceased patient's personal representative, estate executor, or spouse
- a deceased patient's relative or an adult who had a close personal relationship with the patient
- a deceased patient's substitute decision-maker identified in accordance with the *Human Tissue Donation Act*

(See HIA s.25, *Exercise of rights by other persons*; Health Information Regulations s.4)

People under the age of 19 may be mature enough to make their own decisions about their health information. The custodian must determine if a person has the capacity to understand his or her rights and the consequences of exercising these rights. If someone under the age of 19 has the capacity to make routine decisions about his or her personal health information, custodians may consider this person to be a mature minor. Keep in mind that the HIA refers to the collection, use, and sharing of personal health information, not treatment decisions.

A custodian who has reasonable doubt that a patient is a mature minor can assume that the

patient's guardian or parent will be making decisions on the patient's behalf. The custodian should discuss this with the patient before sharing the patient's information.

A custodian should share a patient's personal health information with the substitute decision-maker on a need-to-know basis, and only for the stated purpose.

Example

Anne, age 15, tells a nurse practitioner at the health centre that she is sexually active and wants a prescription for oral contraceptives. The nurse practitioner decides that Anne has the capacity to consent to sharing her information in order to have a prescription filled. Anne asks the health centre not to inform her parents, and this express instruction is noted in her medical records.

When Anne is diagnosed with melanoma several months later, the physician at the health centre decides she does not have the capacity to fully understand how her information will be shared with the various agencies and health service providers who will make up her cancer care team. In this case, the physician will disclose the melanoma diagnosis and treatment information to Anne's parents, even if she objects. Anne's parents will not be told that she is taking contraceptives because that information is not relevant to the care she is currently receiving and the health centre does not have Anne's consent as a mature minor to share the information.

Substitute decision-makers are required by the HIA to consider the wishes and beliefs of the patient and to weigh the benefits against the risks before making decisions on that person's behalf.

(See HIA s.26, *Duty of substitute decision maker*.)

Knowledgeable Consent

Consent is knowledgeable if patients know:

- why and how their personal health information will be collected, used, and shared; and
- they may provide or withhold their consent.

(See HIA s.14, *Interpretation: knowledgeable consent.*)

When custodians and agents collect personal health information from patients, they must inform them how their information may be collected, used, or shared. Nurses, nurse practitioners, physicians, and pharmacists may find it necessary to explain privacy laws to their patients more than once and in more than one way. Custodians and agents may find it useful to tell patients how their information will be protected.

Develop reasonable options for providing notice to patients in your health care organization. If something is likely to be true most of the time for most people in a similar situation, it is reasonable to assume that this same thing would apply to other people in a similar situation. Notices about how patients' health information may be collected, used, or shared could include posters, pamphlets, and short videos. These should be placed where patients will see or hear them.

(See HIA s.15(2), *Notice: purposes of collection, use or disclosure.*)

If there is any possibility that a patient did not see or understand the notices, the custodian must provide additional informative materials or explain them to the patient. The more important a question or situation is, the more important it is to make sure a patient understands it. When you tell patients how their information may be collected, used, or shared, ask them to repeat what they have heard or what they understand you have said, rather than just asking, "Do you understand?"

Example

While he was waiting in the reception area before being admitted to the hospital, Mike watched a short video on closed-circuit TV. It showed common examples of how patients' health information is collected, used, and shared.

A clerk at reception completes the hospital registration process with Mike. She includes a health information collection notice. She asks Mike, "May we send a summary of this hospital visit to your family physician or community health nurse so they can provide follow-up care? If so, please give us the name of your physician or health centre."

Mike tells the nurse his physician's name because he understands why it is important for the physician to have information about his treatment at the hospital.

Elements of a Valid Consent

According to the HIA, a valid consent for the collection, use, or disclosure of personal health information must be:

- given by the individual concerned
- related to the information to be collected
- knowledgeable
- not obtained through deception or coercion

(See HIA s.15(1), *Elements of consent.*)

A valid consent clearly identifies the individual and is given by that person or a substitute decision-maker.

Before giving his or her consent, the patient must be told why the personal health information is being collected, used, or shared. A custodian or agent must identify the risks and benefits of consenting. The patient must consent voluntarily and must be aware that she or he can withdraw the consent.



Note: Public Health notification is required in the case of reportable and notifiable diseases and procedures. Patient consent is not required because patients cannot withhold consent in these cases. However, they should be informed before their health information is disclosed so there will be no surprises. The practice of informing the patient should be applied in other cases of information sharing, even if consent is not required by law.

Implied and express consent are discussed in the following sections.

Implied Consent

If a patient provides information and a custodian believes the patient knows how the information may be used, the custodian can assume that the patient has consented to the collection, use, and disclosure of that information. This is known as implied consent.

Custodians and agents must have a patient's implied consent when they collect information in order to deliver a health service. They can assume they have this consent if they've provided notice as described above, the patient seems knowledgeable, and the patient has given them personal health information. Custodians and agents can also assume they have the patient's implied consent if they collected the patient's information from a health service provider who provided notice, as above, and received the patient's knowledgeable consent.

It is very important to make sure patients understand that they have the right **not** to consent to sharing their personal health information. They also have the right to set limits when collecting, using, or sharing their information is not required by law.

An implied consent does not require a signature. Other forms of identity verification are used, such as asking patients to confirm their registration information when they arrive for an appointment. Patients may also be identified by any two of the following:

- a photo ID card, such as a valid driver's license
- a valid health care card with a health care number tied to the patient's name
- two witnesses confirming the patient's identity
- the wristband on a hospitalized patient

Two pieces of identifying information may be obtained from a patient's wristband. A patient's room number cannot be used to identify the patient.

Once consent has been obtained, it is not necessary to request it again every time information is shared with other health service providers in order to provide continuing care and treatment. It also is not necessary to request consent again when information is shared between custodians for uses that are allowed under *Part 4 Collection, Use, Disclosure and Protection of Personal Health Information* of the HIA.

Example

A physician orders routine laboratory tests for Judy. It is reasonable to assume that Judy has consented to giving her personal health information to the laboratory.

Custodians cannot assume that a patient has provided implied consent if they know the patient never consented or withdrew consent to having the information collected. Custodians also cannot assume consent if they know a patient has expressly instructed that her or his information should not be shared.

(See HIA s.17–19 for more information about implied consent.)

Following are some examples of implied consent.

Examples

A patient is referred to a non-government health care provider for treatment.

A patient makes a complaint to the DHSS about a health service that was provided or not provided to him. An HSSA can share information with the Department without a consent form signed by the patient if the Department needs the information to resolve the complaint (HIA s.62). (Note that express consent is required to share information with a Member of the Legislative Assembly.)

A patient admitted to Stanton Territorial Hospital is being transferred to Alberta for continued care. Implied consent allows Stanton to share information with the patient's care team in Alberta.

A child is being assessed by the Stanton Child Development Team. Some results will be shared with the NWT Office of the Chief Public Health Officer (OCPHO). No consent is required to share information with the OCPHO.

Personal health information collected in order to provide a health service may be used for other purposes set out in the HIA. These purposes include verifying billing and benefits eligibility, forwarding information to another health service provider, internal and health system management, and health promotion.

A custodian (e.g., the DHSS) that collects information from another custodian (e.g., a HSSA) for one of the authorized uses set out in Part 4 of the HIA can assume that the patient provided implied consent for that use. The HIA allows the first custodian to give information to another custodian, and so on, unless the patient has given express instructions limiting the sharing or use of that information.

Examples

Bill goes to the lab to have a blood sample taken for testing. Some of the sample is processed at the local laboratory and some is sent to an Alberta laboratory. Bill's implied consent to share his personal health information for the purpose of receiving a health service applies to both the local laboratory and the Alberta laboratory.

Bill's physician must make sure Bill has not expressly withheld consent to sending his blood sample to both laboratories.

During a check-up Bill, who has diabetes, tells his physician he smokes. The physician records this information in Bill's chart.

The DHSS is developing tobacco cessation programs and wonders whether a program should focus on people with diabetes. The DHSS asks the physician how many of his diabetic patients smoke. The physician uses patients' charts to determine the number and report it to the DHSS. Consent from patients is not required because the HIA s.43(2) allows a public custodian to disclose information to another public custodian for the purpose of health system planning.

Express Consent

Express consent is required before a patient's personal health information can be collected, used, or shared in circumstances that are not specifically allowed by the HIA or other legislation. Express consent must be written unless a patient is unable to write for a reason such as illiteracy or physical disability.

A written express consent must:

- Identify the individual the personal health information is about.
- Include a statement that the individual:
 - knows the purposes of the collection, use, or disclosure of the personal health information;
 - consents to the collection, use, or disclosure of the information;
 - knows that she or he may withhold consent;
 - knows that he or she may withdraw consent.
- Be signed or include the electronic signature of the individual.
- Be dated.

(See HIA s.20(3), Requirements: written form.)

If a patient is unable to write an express consent, the custodian can accept a verbal express consent. The custodian must record the verbal express consent in writing as soon as possible, including the reason why the patient could not write a consent. This document is placed in the patient's file. The entry must clearly identify the custodian or agent who recorded the verbal consent and the date the consent was provided. It must be dated and signed by the custodian or agent.

(See HIA s.20(2), Exception: verbal form.)

The use of recorded verbal express consents should be limited. This option should not be used if there is no way to authenticate the identity of the person giving the verbal express consent. It should not be used because it is more convenient than obtaining a written consent.

A custodian can assume a recorded express consent is valid.

(See HIA s.21, Reliance on record of consent.)

The following are some examples of express consent.

Examples

Stanton Hospital Foundation is raising money for a new piece of equipment. It wants to appeal for donations from people who received health services at the hospital. It can only contact people who signed express consents that allow the foundation to contact them.

A community breastfeeding group set up to support new moms. It asks the health centre for their names. The centre can provide their names because it obtained written express consents from new moms at its well-baby clinic to release their contact information to the breastfeeding group.

A child is assessed by the speech language pathologist. It would be helpful for the child's teacher to have the assessment results in order to continue to support the child. The speech language pathologist asks the child's parent to provide a written consent for release of information to the teacher.

Sam asks a Member of the Legislative Assembly to help him resolve a conflict with his HSSA. The MLA requests information about the situation from the HSSA. The Authority tells the MLA it cannot release Sam's medical records to him until Sam signs an express consent.

A research ethics committee may require custodians to obtain express consent before sharing patients' information with researchers.

(See HIA, Part 4.)

Example

A physician has received Research Ethics Committee (REC) approval for a research study. The REC requires the physician to obtain express consent from each participant.

Ayla is a patient at the medical clinic. The physician asks Ayla if she wants to participate in a research study. He tells Ayla she does not have to participate in the study. She will be treated at the clinic whether or not she is in the study.

If Ayla decides to participate in the study, she will provide express consent to sharing her personal health information with the researcher.

(See HIA s.20, Form of express consent.)

Consent Conditions and Express Instructions

The HIA allows patients to state that they do not want their personal health information to be shared. Patients also can limit the amount or type of information that can be shared or with whom it can be shared. These limits are called consent conditions.

According to the HIA s.22, consent conditions include express instructions. For example, an express instruction in a patient's medical record may state that personal health information must not be shared with family members or a community counsellor.

Express instructions cannot be ignored. The custodian must have consistent practices in place to make sure a patient's express instructions will be seen by anyone who accesses that patient's

record. A clinic may flag the express instructions on the face sheet of a paper chart, as an alert in demographics in the central patient registry, or as an alert in an electronic health information system.

A custodian who is given consent conditions by a patient must do the following:

- Tell the patient the implications of making such conditions, if there are any.
- Take reasonable steps to comply with the conditions.
- Record the conditions.
- Notify anyone to whom the custodian discloses the information.

A patient may specify consent conditions limiting the information that one custodian can give to another. As a result, the custodian or agent cannot disclose all the information another provider might need in order to care for the patient properly. In this case, the custodian or agent must tell the other provider that the patient's personal information is incomplete due to a consent condition.

Example

Mike's leg was broken in three places when he fell from a ladder while painting his house. The primary care physician refers him to an orthopedic surgeon. Mike asks the physician not to tell the surgeon that he has a history of addictions to prescription drugs. The physician tells Mike the possible consequences of not sharing this information: he might not receive appropriate and safe care, or the surgeon might refuse to treat him.

The physician must decide whether it is important for the surgeon to have this information. She thinks the information is necessary; therefore, she must inform the surgeon that Mike's record is not complete.

(See HIA s.23, Duty to give notice if disclosure limited.)

Note, however, that a health service provider may be required to share a patient's health information without the patient's consent. Conditions placed on consent by a patient are not retroactive and do not take effect in the following circumstances:

- The patient's information is required by law (e.g., a requirement to notify the RCMP in the case of a gunshot wound).
- The information is required by established professional standards of practice.
- The information is required by a Prescription Monitoring Program.

Sometimes a custodian will not be able to comply with the conditions. For example, a patient may specifically instruct that personal information be "masked" or hidden from view in an electronic health information system. If the custodian's system does not have the technical capacity to mask the information or if it is considered not within professional standards to mask that information, the custodian will not be required to meet the condition. However, the custodian should discuss the situation with the patient and take other measures to protect the patient's information and respond to the patient's concerns.

Withdrawal of Consent

Patients can change their minds about having their personal health information shared. In this case, the patient must give the custodian a written notice of withdrawal of consent. The withdrawal of consent, with any conditions placed on the consent (partial or full withdrawal), is dated and maintained in the patient's record. The original consent is not removed or deleted. This process is similar to that used to correct an entry in a patient record.

Withdrawal of consent by a patient is not retroactive and does not take effect in the following circumstances:

- The patient's information is required by law (e.g., a requirement to notify the RCMP in the case of a gunshot wound).
- The information is required by established professional standards of practice.
- The information is required by a Prescription Monitoring Program.

When a patient withdraws consent, the custodian receiving the notice must:

- Tell the patient the implications of withdrawing consent, if there are any.
- Take reasonable steps to comply with the withdrawal.
- Record the withdrawal.
- Notify anyone to whom the custodian disclosed the information during the previous year.

Remember that whenever you disclose information about a patient you must record the disclosure in the patient record. If a patient withdraws consent, disclosures must be easy to track so you can notify everyone who received the patient's information.

Since withdrawal of consent is not retroactive, the custodian is not required to ask recipients to return or destroy information about the patient.

(See HIA s.24, Withdrawal of consent.)

Resources

These resources and templates are available at the end of the HIA Guide. Click on the hyperlink or use the bookmarks to view them.

Notification of Collection of Personal Health Information

Sample notices you can customize and use in your organization.

These resources are available from DHSS website [health-privacy-protecting-your-health-information](http://www.hss.gov.nt.ca/health/slides/health-privacy-protecting-your-health-information) (<http://www.hss.gov.nt.ca/health/slides/health-privacy-protecting-your-health-information>)

Consent – Video

Additional Resources

Accreditation Canada. (2015). *Required Organizational Practices: Handbook 2015*. Retrieved from <http://www accreditation.ca/sites/default/files/rop-handbook-en.pdf>

Chapter 3. Consent – Test Your Knowledge

The following quiz applies many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 172](#).

1. Mary sees a physician at her HSSA. The physician refers Mary to a specialist physician at another HSSA facility. What type of consent is required?
 - a. implied consent
 - b. express consent
2. Bob's physician writes a referral letter to the private physiotherapist on Bob's behalf and sends the letter by fax. What type of consent is required?
 - a. implied consent
 - b. express consent
3. Which of the following are criteria for elements of valid consent?
 - a. legal authority, validity expiration date, patient's email address
 - b. consent of individual, relates to the information, knowledgeable, and not obtained through deception
 - c. identity of patient, purpose of the disclosure, patient's acknowledgment
 - d. patient's address, information release date, patient's acknowledgment
4. Patients have the right to determine who has access to their personal health information and to set limits on the collection, use, and sharing of that information.
 - a. true
 - b. false
5. Express consent can be either written or verbal.
 - a. true
 - b. false

Chapter 3. Consent – Summary of Key Concepts

1. **Substitute decision-makers** act on behalf of patients who are unable to make their own choices about their health information. They include parents, guardians, trustees, legal representatives, and people named in patients' personal directives.
2. **Knowledgeable consent** means patients know why and how their personal health information will be collected, used, and shared. They are aware that they have the right not to share their information.
3. A **valid consent** must be:
 - given by the individual concerned
 - related to the information to be collected
 - knowledgeable
 - not obtained through deception or coercion
4. If a patient provides information and a custodian believes the patient knows how the information may be used, the custodian can assume that it has the patient's **implied consent** to collect, use, and disclose the personal health information necessary to deliver a health service and for authorized (secondary) uses set out in the HIA.
5. A patient must give **express consent** before personal health information can be shared in ways that are not specifically allowed by the HIA or other legislation.
6. Patients have the right to set **consent conditions** and **express instructions** that limit or control how their personal health information will be used and shared.
7. A patient who changes his or her mind about sharing personal health information can give the custodian a written notice of **withdrawal of consent**.

4 Collection

Introduction

Patients trust health information custodians with their personal health information. They expect custodians to act in their best interests and safely manage this information. The *Health Information Act* (HIA) specifies what custodians must do when they collect personal health information.

(See HIA s.27. Custodian required to comply.)

This chapter includes the following **key concepts**:

1. Basic privacy principles
2. When you can collect personal health information
3. Collecting information from third parties
4. Required notice
5. Patient identifiers

Basic Privacy Principles

Whenever you collect, use, or share personal health information, remember:

1. Do not collect identifiable information if non-identifiable information will do.
(See HIA s.28(1), Restriction: non-identifying information.)
2. Do not collect more personal health information than is necessary for the purpose which you are collecting it.
(See HIA s.28(2), Extent of information.)

Even if the HIA lets you collect, use, and share information, it doesn't mean you always should. The collection, use, and share still must abide by these principles.

"Just because you can, doesn't mean you should."

When you collect information, you are responsible for keeping it confidential and secure. The less information you collect, the easier it is to protect.

When You Can Collect Information

A custodian or agent can collect personal health information under the following conditions:

- The patient has consented or
- The collection is allowed by the HIA or another Act or
- The HIA or another Act allows someone to share the information with the custodian.

(See HIA s.29, Collection: general.)

Custodians and agents can collect personal health information in a manner and for the purposes set out in HIA s.30, 35-37.

Collecting Information from Third Parties

Most of the time, it is best to ask patients directly for their personal health information. However, we sometimes need to collect information from other sources. Following are examples of when this might happen.

- The patient allows the custodian to ask another person for the information. The patient's consent may be written or verbal. The other person does not have to be the individual's substitute decision-maker.
- Information is collected from a health service provider in order to care for the patient or support the delivery of a health service.
- It is not possible to obtain information from the patient.

Example

Mary is unconscious when she is admitted to the hospital. Her friend Mike came to the hospital with her. The doctor asks Mike if he knows what Mary was doing before she lost consciousness and he called for help. The doctor asks other questions about Mary's health history.

- Collecting information from the patient could prejudice the health or safety of the patient or someone else; or
- Information given by the patient might not be accurate.

Example

David has fainting spells but does not tell his doctor. He knows his doctor could notify the Registrar of Motor Vehicles. David is afraid of losing his driver's license.

David's wife tells the doctor she thinks David should not be driving. The doctor would be justified in collecting information from David's wife because David appears to be concealing health problems that could lead to accidents.

- The information is necessary to see if that patient is eligible for a health service or benefit.
- Family history information is needed in order to care for a patient.

Example

Richard, age 45, has symptoms of early-onset Alzheimer Disease. The doctor asks Richard's brother if anyone else in the family has had this disease.

- The HIA or another law requires or allows the custodian to collect the patient's information from another person.
- A research ethics committee allows the custodian to collect the patient's information from another person.

Always consider the source of health information you use. Some sources are more reliable than others. You must also make sure the source of the information has the legal authority to collect and disclose the information. If the source providing information does not have the legal authority to disclose the information, you cannot collect the information.

(See HIA s.30, *Collection from other source*.)



(For more information on what consent is needed to collect information from third parties, see [Chapter 3, Consent](#).)

Required Notice

Before obtaining personal health information from a patient or substitute decision-maker, the custodian must inform the patient or substitute decision-maker:

- what laws allow the custodian to collect the information
- why and how the information may be used
- the patient's right to withhold or withdraw consent or place conditions on the consent
- why and to whom the custodian may share the information
- how to get in touch with the designated contact person if the patient has questions

A custodian who does not notify the patient of the information listed above cannot assume she or he has the patient's implied consent to collect, use, and share the information.

(See HIA s.31, *Duty to provide information*.)



(For more information on ways to provide notice, see [Chapter 2, Custodians and Agents](#).)



(For more information, see [Resources, Notification of Collection of Personal Health Information](#).)

Patient Identifiers

Ask for at least two patient identifiers before collecting personal health information from a patient and before providing a patient access to her or his personal health information. Failure to correctly identify patients can lead to serious problems such as medication errors, as well as privacy breaches. The following identifiers are acceptable:

- a photo ID card, such as a driver's license
- a valid health care card showing a patient's health care card number

- two witnesses confirming the patient's identity
- the wristband on a hospitalized patient

Get into the habit of asking patients for photo ID whenever they visit your facility. This is especially important when people first register for health services, but make it a common practice so no one feels singled out. This applies to everyone, including patients who live outside the Northwest Territories.

When we verify the identity of a patient we are preventing treatment errors and ensuring the integrity and confidentiality of the information in the medical record.

Don't photocopy the patient's ID or record a driver's license number – only verify that the picture on the card looks like the person at the desk. Confirm the spelling of the patient's name and his or her date of birth.



A personal health number is the key to a patient's health information. Personal health numbers are protected under the HIA.

When a patient presents her or his card in order to obtain health services, carefully check the health care number and the registration details. Ask to see photo identification or other identifiers to make sure the health card belongs to the person who shows it to you.

These are the **only** people who can collect or use a patient's health care number:

- the patient
- a custodian or the custodian's agent
- a person to whom the custodian has disclosed the number
- a person who is permitted by another act to collect or use the number

Doctors, laboratories, pharmacies, and other health services providers use patients' personal health numbers to keep complete and accurate health records.

(See HIA s32(1), Prohibition: personal health number.)

A person other than a health information custodian who asks a patient to provide a personal health number must tell the patient why she or he is authorized to have it.

(See HIA s.32(2), Requirement to provide information.)

Collection with Recording Device

Personal health information may be collected using a voice recorder, camera, or other device. The custodian or agent must explain that the device will be used before collecting the information.

It is a good idea to get a written consent to make sure the patient understands why information will be collected and that it will be used and stored.

Make sure good safeguards are in place to protect the security of personal health information. Use recording equipment that is owned and controlled by the custodian and treat the record in the same way you would any other medical record.

(See HIA s.33, Recording device.)

Resources

The following resource is available at the end of the HIA Guide. Click on the hyperlink or use the bookmarks to view it.

[Sample Consent to be Photographed/Recorded](#)

Before a health information custodian collects personal health information using a recording device, the custodian must tell the patient that the device will be used.

Chapter 4. Collection – Test Your Knowledge

The following quiz applies to many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 173](#).

1. Who are the people who collect personal health information and have a special responsibility to manage the private information provided to them?
 - a. patients
 - b. custodians
 - c. other patient's family
2. Which term refers to gathering, acquiring, receiving, or obtaining health information from an individual?
 - a. use
 - b. collection
 - c. sharing
3. Which of the following people are authorized to collect or use a patient's health care number?
 - a. the patient
 - b. a custodian or the custodian's agent
 - c. an adventure tour company
 - d. a community pharmacist

Chapter 4. Collection – Summary of Key Concepts

1. Whenever you collect, use, or share personal health information, remember:
 - Do not collect identifiable information if non-identifiable information will do.
 - Do not collect more personal health information than is necessary for the purpose which you are collecting it
2. A custodian can collect personal health information under the following **conditions**:
 - The patient has consented.
 - The collection is allowed by the HIA or another Act.
 - The HIA or another Act allows someone to share the information with the custodian.
3. If possible, collect information directly from the **patient**. If necessary, information can be collected from a **third party** that has the legal authority to disclose information about the patient.
4. Patients must be **notified** of their privacy rights and how their information may be used and shared before their personal health information is collected.
5. Ask for at least two **patient identifiers** before collecting personal health information from a patient and before providing a patient access to her or his personal health information.

5 Use

Introduction

Patients give information to health service providers in order to obtain treatment. They expect that their personal information will be used for that purpose. If a custodian or agent will use the patient's personal health information for other purposes, these uses must be explained to the patient.

This chapter includes the following **key concepts**:

1. Basic privacy principles
2. When you can use personal health information
3. De-identifying personal health information
4. Data matching using personal health information
5. Additional uses of health information by public custodians

Basic Privacy Principles

To use personal health information is to handle or apply information for a purpose. It does not include disclosure of the information.

Do not use identifiable information if non-identifiable information will do.

(See HIA s.28(1), *Restriction, non-identifying information.*)

Do not use more personal health information than is necessary for the purpose for which you are using it.

(See HIA s.28(2), *Extent of information.*)

A custodian may use personal health information to provide health services. This may also include appropriate and authorized access to and sharing of personal health information by a custodian or their agent for the purposes of providing health services or for health system management.

When You Can Use Personal Health Information

Personal health information may be used by a custodian **only** when:

1. The person has consented to that use, or

Example

A long-term care facility operated by the HSSA collects personal health information about a resident. The resident allows the facility to use the information to develop health care plans and provide services for the resident.

2. The use is permitted or required by the HIA or another NWT Act or an Act or regulation of Canada, or

Example

Under the *Hospital Insurance and Health and Social Services Administration Act*, agents at Stanton Territorial Health Authority who hold a statutory appointment under that Act may use patient information as part of a quality assurance activity.

3. The HIA or another NWT Act or an Act or regulation of Canada permits or requires a person or organization to disclose the information to the custodian without the express consent of the individual the information is about.

(See HIA s.34, *Use: general.*)

Authorized (Secondary) Uses of Health Information Allowed by the HIA

The HIA allows health information custodians to use personal health information for the following reasons:

- to provide health services
- to determine or verify the eligibility of the patient to participate in a program of the custodian or to receive a health service, benefit or related product
- for the purpose for which it was collected and any related functions necessary to achieve that purpose
- for internal management purposes, including resource allocation, evaluation, quality improvement, processing payments, training, planning, policy and procedure development, chart auditing, legal services, error management services (such as Canadian Medical Protective Association support) and risk management services.

Examples

The pharmacy wants to know what type of public awareness materials should be created to improve its services. The data analyst runs a report from the billing information to prepare the list of prescriptions dispensed most frequently. Individual patient information is de-identified in the list; only aggregate information is used for internal management purposes.

- to carry out an inspection, investigation or review of a health facility
- to do research in accordance with the research requirements of the HIA
- to ask for a patient's consent, for example in order to give the patient's information to a researcher

Example

Doctor Cardinal uses hospital records to obtain the names and contact information of patients who have lung cancer. She contacts these patients to ask if they would consent to having their personal health information used by a researcher who is studying the extent of this disease in the NWT.

- to produce non-identifiable data (See De-Identifying Health Information, below.)
- to comply with a law or court order
- to educate health service providers, such as resident physicians and student midwives while mentored on the job.

(See HIA s. 35, Use by custodian.)

De-Identifying Health Information

Custodians may strip and transform personal health information to make it non-identifiable data in accordance with established de-identification procedures that address re-identification risks.

(See HIA s.36(1), Transformation of information; Health Information Regulations s.13(1)(a).)

Example

A study by DHSS to predict the demand for immunization services requires statistical information from current patient records. The data is extracted from electronic health information systems and turned into aggregate data that is non-identifying.

Only a few data elements are needed in order to identify an individual person. De-identifying patient records requires careful planning. Custodian policies on the use of personal health information should include steps to consider both the type of data and the size of the study to ensure that personal health information is protected. Also consider the risk of re-identifying the health information after the information has been made available. See the resources for recommended de-identification guidelines.



(See the [Resources listing at the end of this chapter.](#))

Data Matching

Custodians may match data from two or more data sources (e.g., paper patient records, billing records, laboratory test results, and electronic patient records) if they have properly collected the information. They must use the information for a purpose authorized by the HIA.

Data matching is often used to make sure patient records are complete and for data integrity by confirming information is added to the correct medical record. Information may be compiled about registration, diagnoses, treatment, and care. Unique identifiers, (name, date of birth, and health care card number) are used to make sure personal health information is entered in the right electronic or paper medical record. The HIA allows technology such as an Enterprise Master Patient Index (EMPI) which joins records from more than one electronic health information system and links these to the same patient.

(See HIA s.36(2), Data matching.)

Additional Uses of Health Information by Public Custodians

The DHSS and HSSAs can also use personal health information:

- for health system planning and management, including to
 - develop, manage, and plan health programs and services
 - plan and allocate resources
 - evaluate and monitor health services
- for public health promotion and public health surveillance
- to administer and enforce the HIA

Example

The DHSS may use data collected under the HIA to report on the number of patients admitted to hospitals with flu symptoms and to monitor the efficacy of the flu immunization program.

(See HIA s.37, Additional uses by public custodian.)

Resources

These resources and templates are available at the end of the HIA Guide. Click on the hyperlink or use the bookmarks to view them.

Use of Personal Health Information at-a-Glance

Use this guide to assist you to respond to frequently asked questions (FAQ) regarding the use of personal health information for authorized (secondary) uses.

These resources are available from DHSS website [health-privacy-protecting-your-health-information](http://health-privacy-protecting-your-health-information.ca).

Recommended de-identification guidelines

The following publications are available online:

Canada Health Infoway. (2012). *Tools for De-Identification of Personal Health Information*. Retrieved from <https://www.infoway-inforoute.ca/en/component/edocman/supporting-documents/500-tools-for-de-identification-of-personal-health-information>

Canadian Institute for Health Information. (2010). *“Best Practice” Guidelines for Managing the Disclosure of De-Identified Health Information*. Retrieved from <http://www.ehealthinformation.ca/wp-content/uploads/2014/08/2011-Best-Practice-Guidelines-for-Managing-the-Disclosure-of-De-Identificatied-Health-Info.pdf>

Canada. Office of the Privacy Commission. (2007). *Pan-Canadian De-Identification Guidelines for Personal Health Information*. Retrieved from https://www.priv.gc.ca/resource/cp/2006-2007/p_200607_04_e.asp

Chapter 5. Use – Test Your Knowledge

The following quiz applies to many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 174](#).

1. Which of the following statements is **false**?

A custodian may use personal health information for the following reasons:

- a. to provide health services
- b. to do research in accordance with the research requirements of the HIA
- c. to make money by selling the health information collected
- d. to comply with a law or court order

2. When can a custodian use personal health information?

- a. The custodian has the patient's consent to use the information.
- b. The use is permitted or required by the HIA or another Act of the NWT or an Act or regulation of Canada.
- c. The HIA or another Act of the NWT or Act or regulation of Canada permits or requires a person or organization to disclose the information to the custodian without the express consent of the individual the information is about.
- d. all of the above.
- e. none of the above.

3. Custodians may strip and transform personal health information to make it non-identifiable.

- a. true
- b. false

4. Mr. Tatum was involved in a car accident with a drunk driver last Friday. The court has ordered his hospital notes on that day as evidence of his injury from the accident.

How is Mr. Tatum's health information used in this scenario?

- a. to ask for a patient's consent in order to give information to a researcher
- b. to educate health service providers
- c. to comply with a law or court order

5. Data matching is often used to make sure patient records are complete and for data integrity.

- a. true
- b. false

Chapter 5. Use – Summary of Key Concepts

1. Personal health information can be used only when the use is **authorized** by the patient, the HIA, another Act of the NWT, or an Act or regulation of Canada.
2. The HIA allows the following authorized (secondary) **uses** of patients' personal health information by custodians and agents:
 - to provide health services
 - to determine or verify eligibility to receive a health program, service or benefit
 - for internal management purposes including
 - billing
 - planning and resource allocation
 - evaluation
 - quality improvement
 - legal services
 - risk management services
 - error management services
 - training, mentoring and education
 - for an inspection, investigation or review of a health facility
 - for research, subject to HIA research requirements
 - to seek a patient's consent
 - for another specific purpose for which it was collected and any related functions necessary to achieve that purpose only
 - for health system planning and management
 - for health promotion and public health surveillance
 - to administer and enforce the HIA.
3. Custodians can **de-identify** personal health information so that it can be used for purposes such as research and statistical analysis.
4. The HIA allows **data matching** (matching personal health information from two or more data sources).

6 Disclosure

Introduction

Personal health information must be protected. Take time to make sure you are disclosing **the right information at the right time to the right person**.

This chapter includes the following **key concepts**:

1. Basic privacy principles
2. When you can disclose personal health information
3. Discretionary disclosures
4. Mandatory disclosures
5. Authenticating the receiving party
6. Keeping a record of disclosures

Basic Privacy Principles

Disclosure occurs when personal health information is shared in any format, whether verbally, electronically, or in hard copy. Patients' personal health information must not be shared unless it is required to provide health services or for another purpose allowed or required by either the patient or by law.

Do not disclose identifiable information if non-identifiable information will do.

(See HIA s.28(1), Restriction, non-identifying information.)

Disclose the least amount of information needed. Do not disclose more personal health information than is necessary for the purpose for which you are disclosing it.

(See HIA s.28(2), Extent of information.)

When You Can Disclose

Personal health information may be disclosed by the custodian only when:

1. The person consents to sharing the information. This includes a patient's implied consent to having his or her information shared for the purpose of obtaining continuing care and treatment from health service providers. A patient also can give express consent to allow other people to access his or her personal health information.
2. The disclosure is allowed or required by law.

Patients have the right to set limits on the sharing of their health information.

Sometimes, the custodian has the discretion to disclose information (**discretionary** disclosure). Other times, the custodian must disclose information (**mandatory** disclosure), if disclosure is required by law.

Discretionary Disclosures

Patients may limit the amount of their personal health information that is shared. They also can decide who may receive their information.



(See [Chapter 3, Consent.](#))

The HIA sets out when a custodian may disclose information. The custodian shall determine if it is necessary to disclose the information in each case. The custodian should consider if the disclosure of the information goes against specific consent conditions and express instructions set by the patient. If so, the custodian must comply within reason with those conditions and instructions. The custodian must attempt to apply discretion in a consistent manner that is reasonable in the circumstances.

Custodians can share patients' personal health information with another custodian for any of the authorized (secondary) uses identified in Chapter 5.



(See [Chapter 5, Use.](#))

(See HIA s.35, Use by custodian; s.37, Additional uses by public custodian; s.43, Disclosure to custodian.)

Custodians can share information with outside facilities that are providing health services to a patient. Custodians can share information with people who are not health service employees if this is necessary to provide continuing care. The custodian cannot share the information in the above circumstances if it goes against the express instructions of the patient.

Examples

Ayla has been discharged from the hospital after surgery. Her friend William is helping Ayla at home while she is recovering. William phones the hospital to ask a question about changing Ayla's bandages.

The charge nurse asks William for Ayla's full name and confirms that William is noted on Ayla's chart as the person who will be helping her at home. The nurse makes sure that Ayla has not given express instructions not to share information with William.

The charge nurse has taken reasonable steps to confirm William's identity and that he is providing continuing care to Ayla. The nurse provides the information to William.

Larry's physician in Yellowknife refers him to a medical facility in Alberta. The physician discloses Larry's personal health information to the health service providers in Alberta to help them diagnose Larry's illness and provide care and treatment for him.

(See HIA s.44, Disclosure for health services.)

If a patient is injured or incapacitated, the custodian may disclose some personal health information in order to find a potential substitute decision-maker. The information may be disclosed to anyone for this purpose, not just a potential substitute decision maker. A custodian may not disclose this information if the patient has given express instructions that it must not be shared.

(See HIA s.45, Disclosure for contact purposes.)

Sometimes it is reasonable to assume that patients would authorize the disclosure of their personal health information. In the following example, information would be stated in general terms related to the location and condition of the patient on the day when the information is disclosed. The patient did not give an express instruction to the

contrary, and the disclosure is made in accordance with accepted professional practice. This applies only when a patient is in a health facility. The information is given only to people who have a close personal relationship to the patient.

Example

Janet goes to the reception desk at the hospital and identifies herself as the mother of a 17-year-old mature minor, who she understands has been admitted. She gives her son's name, and asks for his location and general condition. The patient has not indicated that he does not wish to be contacted or visited by family.

The hospital would be justified in disclosing the information to Janet.

Remember that information cannot be disclosed, even to family members, if patients ask to have it kept private.

Example

Janet goes to the reception desk at the hospital and identifies herself as the mother of a 17-year-old mature minor, who she understands has been admitted. She gives her son's name, and asks for his location and general condition. Janet's son was conscious when he was admitted. He specifically told the nurse that he did not want his family to know he was in hospital.

The hospital would be justified in withholding information from Janet.

If a caller or visitor says he or she is not a family member, the custodian may make further inquiries to determine if the person has a close personal relationship with the patient.

Section 46 of the HIA allows the discretionary disclosure of personal health information. The release of information is not limited to family members, and not all family members are entitled to receive information. It may not be appropriate, for example, to share information with a patient's mother or estranged spouse.

Before sharing any information, the custodian should ask questions to determine whether a close personal relationship exists between the patient and the person asking for information. The custodian decides whether or not to share information based on facts provided by the patient or the person asking about the patient.

When a patient dies, the custodian has discretion to disclose information about the circumstances of the death or health services recently provided to the individual.

The custodian has discretion to determine the appropriate limited amount of information that is required in the situation. This may include identifying the deceased, informing relatives about the death, or allowing relatives to make informed health decisions.

Custodians can share personal health information about deceased patients for the following reasons:

- to identify the person
- to inform a relative or a person who was in a close personal relationship with the deceased about the patient's death and any recent health services received
- to inform another person about the circumstances of the death
- to enable a personal representative, executor, or spouse to settle the patient's estate
- to allow a relative to make an informed health decision about themselves or their child

- to help a person who has custody of a child who is a relative of the deceased to make informed health decisions about the child (this allows adoptive parents to get information about a child's biological parent if deceased, subject to it being an open adoption.)

A relative is a spouse, including common-law spouse, and anyone related to the patient by blood, adoption, or marriage.

(See HIA s.47 (1), Definition: "relative"; s. 47 (2), Disclosure about deceased individual)

Custodians can disclose personal health information related to the delivery of health services for the following reasons:

- to determine or verify a patient's eligibility to receive a health service or benefit provided by the GNWT or Federal Government
- to determine or provide payment to the custodian for health services or benefits
- to process, monitor, verify or reimburse claims for payment for health services or benefits; or
- to provide payment to or obtain payment from a government department or organization, for health services or benefits provided.

(See HIA s.48, Disclosure: health services delivery.)

Example

The DHSS may use patient information disclosed by an HSSA to determine if a patient is eligible to receive Extended Health Benefits coverage.

Custodians can share personal health information about a patient to an investigator, adjudicator, complaints officer, or board of inquiry investigating a complaint against a health professional. Custodians can decide what information, if any, to disclose, subject to an investigation, complaints officer, or Board of Inquiry having the power to require the production of records under protection of licensing legislation.

(See HIA s.49, Disclosure: disciplinary proceedings.)

A health information custodian may disclose personal health information about an individual:

- if the health information custodian is a party or witness in a legal proceeding
- to comply with a subpoena or warrant
- to comply with the rules of court
- to a proposed or appointed litigation guardian or a patient's legal representative in order to appoint them
- to an appointed litigation guardian or legal representative
- to an official investigator or inspector
- to a quality assurance committee set out in accordance with the *Evidence Act* and *Hospital Insurance and Health and Social Services Administration Act* for a quality assurance activity

This means that diagnostic, treatment, and care information can be disclosed without the patient's consent if it is required for a legal proceeding. Information may be demanded by a subpoena, warrant, or order from a court, person, or organization that has the legal authority to obtain this information.

- A **subpoena** requires someone to be a witness at a court or hearing. It specifies where and when testimony on a certain matter will be required and may also order a person to meet the requirements of a court to disclose information.
- A **subpoena duces tecum** requires someone to bring documents, for example, medical records, that might be admissible before the court. The subpoena should include details so that a respondent can identify the documents required without difficulty.
- A **warrant** is a written judicial authorization to search for and collect information or an object. A warrant can be issued to obtain personal health information, even if that information can be used to identify an individual patient.
- An **order** is a legal command to produce something. In the context of the HIA, it refers to personal health information.

Remember that you must always be careful about the information you disclose, especially if a court order is not very specific. Disclose only the information that is essential to achieve the purpose for which it is requested.

Example – Request without Consent

An RCMP officer asks to see the records of a patient who he believes attended the health centre last week. The officer has the patient's name and date of birth. He does not have the patient's consent to release the information.

The designated contact person asks if the information is required to respond to a life-threatening emergency. The RCMP officer says the information is required as part of an investigation, but there is no imminent threat to the patient or anyone else.

The designated contact person tells the officer she cannot provide any information about the individual at this time. She instructs the officer to get a warrant or subpoena *duces tecum* or written consent from the patient.

Example – Request with Warrant

The RCMP officer returns to the health centre a few days later with a warrant.

The designated contact person asks if the information is required to respond to a life-threatening emergency. The RCMP officer says the information is required as part of an investigation but there is no imminent threat to the patient or anyone else.

The designated contact person tells the RCMP officer she will call him when the information he requested is available.

If a police officer or any other person has a subpoena, warrant, or court order, determine whether this document identifies the information to be provided. For example, a warrant for someone's arrest doesn't require you to release that person's health information. When a subpoena, warrant, or court order is granted in order to obtain an individual's personal health information, the purpose will be clearly stated in the document.

If the scope of the warrant, subpoena, or order includes disclosure of health information, make sure the document was issued by a court that has authority in the NWT. If the scope is unclear, custodians should get legal advice.

If the subpoena, warrant, or order authorizes the custodian to disclose information to the police or other person, that information must be released.

(See HIA s.50, *Disclosure: proceedings*.)

A custodian may share patient health information with a law enforcement agency, including the RCMP, for law enforcement purposes. This would be the case of risk to public safety, emergency, or when timely investigation in best interest of the public.

(See HIA s.57, *Disclosure: law enforcement*.)

A health information custodian may disclose personal health information about an individual to a person in charge of a correctional facility or youth custody facility. This information will help the facility make decisions about arranging health services for an inmate, housing the inmate in the facility, transferring an inmate to another facility or discharging the inmate.

(See HIA s.51, *Disclosure to correctional facility*.)

A health information custodian may disclose patient health information to the head of a mental health facility where a patient is being held involuntarily. This information will help the facility make decisions about arranging health services for the patient or matters such as accommodations or transfer.

(See HIA s.52, *Disclosure to other facilities*.)

Example

Sahtu HSSA may share patient information with psychiatrists at Stanton Territorial Health Authority when a patient is sent from the Sahtu and admitted involuntarily to Stanton Territorial Hospital under the *Mental Health Act*, if the hospital needs the information to arrange for health services for the patient.

A health information custodian may disclose personal health information to auditors and those providing legal, error, and risk management services to the custodian. This would include, for example, the GNWT Internal Audit Bureau, the Office of the Auditor General, legal counsel, the Canadian Medical Protective Association, and the GNWT Risk Management and Insurance Office.

(See HIA s.53, *Disclosure: audit, legal services, risk management*.)

A person or organization that is thinking of taking over another custodian's practice will probably ask for patient health information in order to evaluate that custodian's operations. The custodian may share copies of patient records only when a potential successor signs an agreement:

- to keep the information confidential as long as necessary for the purpose of assessment and evaluation and
- to securely destroy the information as soon as possible.

This disclosure is mostly limited in practice to private physicians and pharmacists. This does not change the records retention requirements of patient medical records.

(See HIA s.54, Disclosure to potential successor.)

A health information custodian may share patient medical records with a custodian that is taking over its business. The custodian transferring the charts to the new custodian must tell patients as soon as possible.

The custodian who collected the information from the patient is responsible for ensuring the confidentiality and security of the patient records and cannot abandon them. This responsibility can be transferred to the new owner with the appropriate safeguards. The custodian who purchases the business should accept responsibility for and custody of the patient records. This should be detailed in a written agreement.

(See HIA s.55, Disclosure to successor.)

A health information custodian may share personal health information with another custodian to prevent fraud, limit abuse of health services, or prevent a crime.

Example

A pharmacist believes that a patient has changed a prescription for controlled substances in order to obtain drugs to sell on the street. The pharmacist shares limited information about the patient to other pharmacists and health centres to notify them that someone may try to fill an illegal prescription.

(See HIA s.56, Disclosure: for prevention of fraud, abuse, offence.)

A health information custodian may disclose personal health information about an individual in order to prevent or reduce an imminent threat or risk of serious harm to anyone's health or safety, or an imminent or serious threat to public safety.

The potential victim(s) must be identifiable. The risk of harm or threat must be serious enough that a reasonable person would believe that harm could occur. To qualify as an imminent threat, a threat must create a sense of urgency.

Example

Connie was beaten up by Al, her common-law husband. She has a concussion and internal injuries. Connie says Al is threatening to kill her when she is released from hospital. The custodian calls the police. Before the police can start an investigation, the custodian will need to disclose Connie's personal information. The HIA allows the custodian to make this disclosure.

Custodians may share personal health information with medical or mental health experts in order to decide whether disclosure could prevent or reduce an imminent threat or risk of serious harm, or whether disclosure to a patient could cause serious harm to the patient.

(See HIA s.58, Disclosure: prevention of harm.)

Custodians may share patient's health information to consult with persons to determine if a patient's access or correction request should be granted.

(See HIA s.59, Disclosure for consultation; s.106(1)(b), Extension of time limit for responding; s.123(1)(b) Extension of time limit for compliance.)

The DHSS may disclose personal health information to the Federal Government, a provincial or territorial government, an Aboriginal government, or a department or agency of these governments if this information is required to manage, monitor, evaluate and develop the health system or health programs and services.

(See HIA s.60, *Disclosure to government health programs and services.*)

The DHSS and HSSAs may share personal health information with the following organizations identified in the *Health Information Regulations*:

- Northwest Territories Bureau of Statistics
- Canadian Institute for Health Information (CIHI)

These organizations use health information to compile and analyze statistical information that helps the DHSS and the governments identified above to manage and evaluate their health programs and services. The DHSS and HSSAs require an **information sharing agreement** (ISA) with the NWT Bureau of Statistics and CIHI before information is disclosed. The agreement must contain a provision prohibiting the further disclosure by the organization of identifiable personal health information without the consent of the individuals whose information is to be disclosed.

(See HIA s.61, *Disclosure to prescribed person or organization; Health Information Regulations s.5.*)



(See [Chapter 8, Information Managers and Information Management Agreements.](#))

Custodians can share information with the Department (i.e., system navigator) if a patient makes a complaint. The Department must notify the patient that this information has been shared.

(See HIA s.62, *Disclosure to Department.*)

Mandatory Disclosures

Custodians must disclose personal health information if required by the HIA or another Act.

Examples

Three children with measles are treated in the clinic where Amy is a nurse practitioner. She notifies the Office of the Chief Public Health Officer, as required by the *NWT Public Health Act*.

Robert arrives at the emergency room with a deep cut in his arm. The friend who drove him to the hospital says Robert was in a knife fight at the bar. Under the *Gunshot and Stab Wound Mandatory Disclosure Act*, hospital staff are required to notify the local RCMP detachment.

(See HIA s.38, *Disclosure: general.*)

Custodians have to share patient health information with public health authorities if a law requires this disclosure in order to protect public health.

Example

Laboratory tests confirm that a patient has tuberculosis, which is a reportable disease. Ellen, a nurse at the health clinic, notifies the Office of the Chief Public Health Officer, as required by the *NWT Public Health Act*.

More specific disclosure for public health is addressed in the *Public Health Act*.

(See HIA s.66, *Other public health authority.*)

A health information custodian must share information with the IPC if the IPC requires it in order to do the job.

(See HIA s. 42, *Disclosure to IPC.*)

The DHSS and the HSSAs must enter personal health information into designated electronic health information systems, such as the electronic medical record (EMR) system.

Disclosure to the following electronic health information systems must occur as those systems become available to a public custodian or an agent of a public custodian.

(See HIA s.63, *Electronic health information system*; *Health Information Regulations* s.6)

Electronic health information systems*:

- Diagnostic Imaging/Picture Archiving and Communication System (DI/PACS)
- Electronic Medical Record System (EMR)
- Enterprise Master Patient Index (EMPI)
- Health Management Information System (HMIS)
- Health Suite
- ICore
- Interoperable Electronic Health Record (IEHR)
- Interoperable Public Health Information System (IPHIS)
- Laboratory Information System (LIS)
- MediGent
- MediPatient
- MediPharm
- ORMED
- Risk Monitor Pro and future Territorial risk management systems
- Vital Statistics System (VSS)

* Systems are designated by the Minister of HSS and the list may change over time, as other systems become available.

Should future HIA regulations prescribe a custodian who compiles or maintains a registry of personal health information to facilitate or improve the provision of health services or to maintain

a Human Tissue Donation Registry, health information custodians must disclose personal health information to that prescribed custodian.

(See HIA s.64, *Information for registry*.)

If a prescription monitoring program is established under *Pharmacy Act Regulations*, custodians will be required to share patient health information with the monitoring program.

(See HIA s.65, *Prescription monitoring program*.)

Authenticating the Recipient

Before disclosing information, you must take reasonable steps to verify that the person or organization to which the information is disclosed is authorized to collect it and is the intended recipient.

Example

Mary is an assistant at a health centre. A dentist in another city calls her. One of the clinic's patients requires dental surgery and can't remember the names of the medications he is taking. The dentist asks Mary to give him this information.

Mary asks the dentist to fax a request with the patient's written consent and the patient's name, date of birth, and health care number. She asks him to use his dental office's stationery. Mary has taken reasonable steps to verify the caller. (She looked up the dentist's name and contact information in the directory). The patient's information on the letter matches the information in the medical clinic's records. When Mary prepares a response to send to the dentist, she uses his full name and the clinic address.

(See HIA s.39, *Duty of custodian*.)

Keeping a Record of Disclosures

Routine sharing of information as part of providing care and treatment does not need a separate disclosure notation. Whenever you share information that is not part of the routine sharing of information, you must note in the patient record that the disclosure occurred and whether or not written consent was needed. This is called a **disclosure note**. It must identify:

- the patient
- a detailed description of the information that was shared
- when and how the information was shared
- the person or organization that was given the information
- who disclosed the information

A patient can request access to the disclosure information. The disclosure note is part of the patient record and must be maintained for the entire retention period of the patient record.

A record of activity created by an e-health information system can be used to support a record of disclosure. Keep in mind that the information that is automatically created in the record of activity may not meet all of the requirements of a complete disclosure record.

Resources

These resources and templates are available at the end of the Health Information Act Guide. Click on the hyperlink or use the bookmarks to view them.

[Disclosure of Personal Health Information at-a-Glance](#)

Use this guide to assist you to respond to frequently asked questions (FAQ) regarding the disclosure of personal health information.

[Disclosure Decision Tree](#)

Use this illustration to assist you to process common requests for disclosure of personal health information with or without the express consent of the patient.

Chapter 6. Disclosure – Test Your Knowledge

The following quiz applies many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 175](#)

1. When you document a disclosure, you must record:
 - a. what was disclosed, to whom, when and purpose of the disclosure
 - b. who made the disclosure and the authority to disclose
 - c. what format was used to disclose, and when
 - d. all of the above
2. A good test to assess if you completely documented the disclosure is to
 - a. Imagine yourself logging into the EMR and see what you can access.
 - b. Imagine how your co-workers would record a disclosure.
 - c. Have a co-worker follow your disclosure notation to successfully re-create the same package of information.
3. When in doubt about how to process a request for information:
 - a. Determine if the individual has provided consent.
 - b. Determine if the request relates to a current life threatening circumstance.
 - c. Don't disclose.
 - d. Ask your supervisor, designated contact person or custodian for assistance.
 - e. All of the above
4. What is a warrant?
 - a. a written judicial authorization to search for and collect information or an object
 - b. a legal command to produce something
 - c. a demand for someone to be a witness at a court or hearing
5. A health information custodian is told to disclose information to a complaints officer reviewing a complaint against a health professional. This is a mandatory disclosure.
 - a. true
 - b. false
6. A public custodian has a request from a patient to not have their clinic information in the EMR. The public custodian has access to the EMR and regularly puts patient clinic information in the EMR. The public custodian can choose not to put this patient's information in the EMR.
 - a. true
 - b. false

Chapter 6. Disclosure – Summary of Key Concepts

1. Personal health information is sensitive. Custodians and agents ensure that they are protecting the privacy, confidentiality, and security of the information. Take the time that you need to share **the right information at the right time to the right person**. Only share what is needed. Don't share identifiable information if the purpose can be fulfilled using de-identified data.
2. If you are not sure if you have permission to disclose patient health information, **discuss** the situation with your supervisor, designated contact person, or custodian.
3. **Discretionary Disclosure:** A custodian **may** disclose information. The custodian cannot share the information in these circumstances if it goes against the **express instructions** of the patient. Discretionary disclosures include disclosure:
 - To another custodian for an authorized (secondary) use
 - To a health service provider inside or outside the NWT, providing care to the patient
 - To any person providing continuing care to the patient, if necessary
 - To contact a substitute decision maker
 - To a person with a close personal relationship to a patient if the patient is in a health facility and the information is general
 - If the patient is deceased, to a relative or person with a close personal relationship to the patient for identification, circumstances around the death, estate, and genetic history purposes
 - For billing, payment, and health services and benefits eligibility verification
 - To a complaints officer, investigator, or other official in the case of a complaint against a health professional
 - Under a subpoena, warrant, or court order
 - To a quality assurance committee, investigator, inspector
 - To a correctional facility or mental health facility
 - To someone carrying out risk management, error management, and legal services for the custodian
 - To an official auditor
 - To a successor or potential successor of a custodian's practice or business
 - To prevent health services fraud
 - For law enforcement purposes
 - To prevent harm
 - To DHSS if DHSS has received a complaint from a patient about health services provided and it is attempting to resolve it
 - For health system planning and to compile and analyze statistical information

4. **Mandatory Disclosure:** A custodian must disclose all or part of the patient's health information. Mandatory disclosures include:
- When required by the HIA or another Act
 - Public health disclosure to another jurisdiction
 - Disclosure to the IPC
 - Disclosure to a prescription monitoring program
 - Disclosure to designated electronic health information systems
5. Before disclosing information, you must take reasonable steps to **verify** that the person or organization to which the information is disclosed is authorized to collect it and is the intended recipient.
6. Whenever you share information without consent, you must **record the disclosure** including:
- name of recipient
 - date
 - purpose
 - description

7 Disclosure for Research and Research Ethics Committee

Introduction

The *Health Information Act* (HIA) includes a robust privacy framework around the collection, use and disclosure of patient's personal health information for research purposes. All research requests must be approved by a research ethics committee (REC). The REC will consider if express consent from patients is required. Patients have a choice about whether to allow their personal health information to be used for research purposes.

The custodian may share patients' personal health information with a researcher. A custodian can be a researcher, in which case they must apply to a research ethics committee and comply with research requirements set out in this chapter.

This chapter includes the following **key concepts**:

1. Research ethics committee
2. Research approval and disclosure process
3. Research agreement requirements

Research Ethics Committee

Under the HIA, approved RECs must be named by the Minister of Health and Social Services. The Minister has designated the Aurora College Research Ethics Committee as an REC under the HIA.

A REC:

- reviews research proposals and approves or rejects them,
- may set conditions,
- may require or not require a researcher to have the express consent of patients to use their information,
- may make recommendations for custodians to consider before sharing patient information, and
- must comply with the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans.

(See HIA s.69, *Role: research ethics committee*; *Health Information Regulations s.7*)

Research Ethics Committee Review and Approval

A researcher cannot:

- collect personal health information held by a custodian in the NWT unless a Minister-designated REC or a REC from another jurisdiction has approved the research proposal,
- collect patient information from a custodian or do research using patient information without the patient's express consent if a REC requires this express consent.

(See HIA s.70, *Prohibition: research*; s.71, *Prohibition: collection and condition*.)

Application to Research Ethics Committee

A researcher must apply to a REC for approval of a research proposal if collecting personal health information from a custodian. The application must include a research proposal that meets the requirements of the REC.

(See HIA s.72, *Application to research ethics committee*.)

Research Ethics Committee Assessment

The REC will review the application and must consider the following:

- if the research can be done without identifiable health information
- if public interest in the research outweighs concerns about the privacy of patient information
- if the researcher is qualified to do the research
- if the researcher's proposed safeguards to protect the patient information are complete and if patients' express consent is necessary
- if the researcher can collect the information from another source
- if the requirement of express consent would be unreasonable, impractical, or not feasible
- if conditions must be met by the researcher

(See HIA s.73, *Factors for assessment*.)

Notice to Researcher

A REC will notify the researcher of its decision and any conditions, including those pertaining to collecting information from another source or requiring express consent. The REC must provide reasons for its decision and must inform the researcher about any recommendations it makes to the custodian.

(See HIA s.74, Notice required.)

Request for Custodian Disclosure

Once the researcher has received approval from the REC, the researcher may ask the custodian to disclose personal health information.

(See HIA s.75, Prohibition: request for disclosure.)

The health information custodian may, but is not required to, decide to share patient information with the researcher.

(See HIA s.76, Disclosure of information for research purposes.)

The researcher must provide to the custodian:

- an application in a form satisfactory to the custodian
- the license from Aurora Research Institute (if required)
- the research proposal
- the REC's decision
- any other information the custodian needs, for example, about express consent, conditions, or recommendations set by the REC, security safeguards, or destruction methods

The researcher must sign a research agreement with the custodian.

(See HIA s.77, Requirements for disclosure: research; s.80, Disclosure agreement: requirements.)

Research Approved by Extra-Territorial Research Ethics Committee

A custodian can share information with a researcher whose proposal was approved by another jurisdiction's REC if the following conditions are met:

- The research is a multi-jurisdictional project.
- The researcher submits to the custodian an application, an Aurora Research Institute license, the research proposal, the REC's decision, and any other information the custodian needs.
- The disclosure is not disallowed by the HIA.
- The researcher enters into a research agreement with the custodian.

(See HIA s.78, Disclosure: approval by extra-territorial research ethics committee.)

Research Agreement Requirements

The custodian and researcher must sign a research agreement. The researcher must agree to follow the HIA; the custodian's standards, policies, and procedures; REC conditions, and privacy and security safeguards and conditions. The agreement must specify:

- how personal health information will be used and disclosed
- how the confidentiality of the information will be protected
- how the privacy of the individuals will be protected
- the administrative, technical, and physical safeguards to be used to protect records that contain the information
- how records will be modified, returned, or destroyed
- any additional conditions that safeguard against the direct or indirect identification of patients, including any removal or destruction of personal identifiers

A researcher must

- follow any conditions set by a REC,
- not publish identifiable information,
- not contact patients unless the custodian first gets the patients' express consent for the researcher to contact them,
- use the patient information only for approved purposes, and
- abide by the research agreement.

(See HIA s.81, *Researcher requirements*.)

The custodian cannot disclose patient information to a researcher until the research agreement is signed and implemented.



(See Resource [Comparison of Information Management Agreements, Information Sharing Agreements, and Research Agreements](#) in the HIA Guide and Chapter 8.)

Patients' Express Consent

If a REC requires the patient's express consent, the custodian cannot share the patient's information with the researcher unless the patient first provides express consent.

After a research agreement is signed, a custodian can contact patients to see if they want to provide express consent to having their information shared with the researcher.

(See HIA s.82(1), *Seeking express consent*.)

The custodian must make the first contact with the patient and give the patient information about the research. The patient is given the opportunity to contact the researcher for more information. The patient provides express consent for the researcher to contact him or her and to have the custodian share their personal health information with the researcher. Whether or not a patient agrees to having their information shared, it does not change how the patient receives health services from the custodian.

(See HIA s.79, *Requirement for express consent*.)

If a researcher wants additional information from patients, the custodian must first get the patients' express consent to have the researcher contact them.

(See HIA s.82(2), *Collection of further details*.)

Example

A researcher has received REC approval to collect personal health information from a pharmacist. The REC has required that before the information can be shared with the researcher, the patients' express consents must be received. The pharmacist must ask patients for their express consents to the disclosure before sharing any information with the researcher.

Research Fees

The custodian can charge the researcher for the costs of sharing the information. The fees cannot be greater than the cost of providing services such as the following:

- locating personal health information and preparing it for disclosure
- copying records containing personal health information
- delivering personal health information to the researcher
- seeking consents

(See HIA s.80, Research agreement requirements; s.82, Seeking express consent.)

Disclosure Requirements – General Requirements

Custodians are required to record disclosures from patient records, if applicable, including disclosures to researchers. The disclosures may be recorded, if applicable on the patients' medical records, in addition to any other record-keeping for the research disclosure.

If a custodian thinks the researcher has not followed the requirements set out in the HIA and the research agreement, the custodian must not share any more information until the custodian is reassured that the researcher is following the requirements.

(See HIA s.83, No further disclosure.)

Resources

These resources and templates are available at the end of the Health Information Act Guide. Click on the hyperlink or use the bookmarks to view them.

[Processing Research Requests at-a-Glance](#)

This quick-tip guide will help you to process research requests for personal health information.

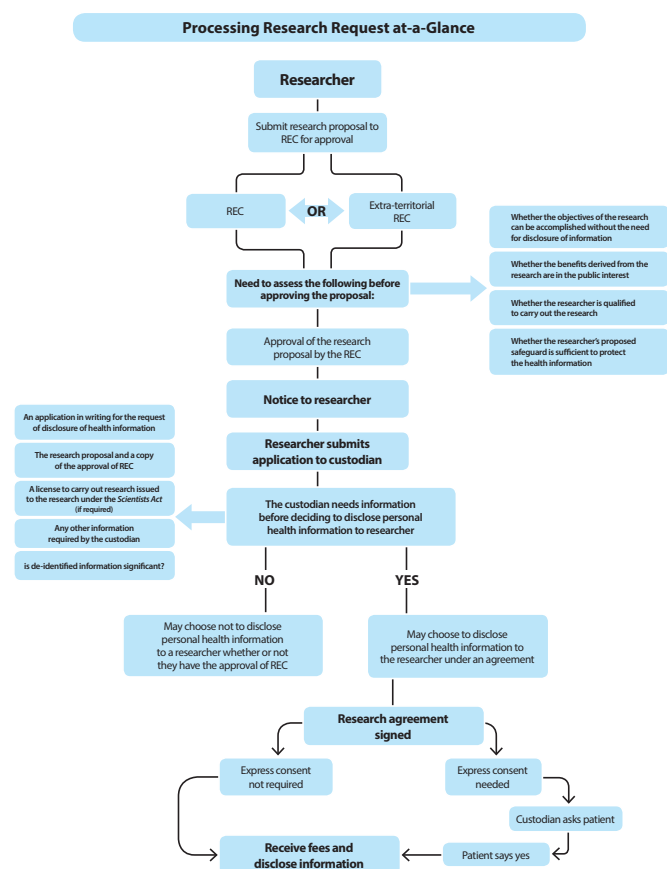
Chapter 7. Disclosure for Research Purposes and Research Ethics Committee – Test Your Knowledge

The following quiz applies many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 176](#).

1. Researchers may contact patients directly to get consent.
 - a. true
 - b. false
2. A research application was not approved by a REC. The researcher can directly ask a custodian to join a research study.
 - a. true
 - b. false
3. A custodian has received an invitation to participate in a research study. What must the researcher provide the custodian?
 - a. a list of patients to contact
 - b. the license from Aurora Research Institute
 - c. the research proposal
 - d. the REC's decision
 - e. the researcher's résumé
 - f. any other information the custodian needs about express consent, conditions, or recommendations set by the REC
4. Which of the following is an agreement between a custodian and a researcher?
 - a. information management agreement
 - b. information sharing agreement
 - c. research agreement

Chapter 7. Disclosure for Research Purposes and Research Ethics Committee – Summary of Key Concepts

1. The Aurora College Research Ethics Committee (REC) is designated the Northwest Territories REC for the purposes of the HIA.
2. Research including personal health information held by a custodian **must have prior REC approval** including research done by a custodian.
3. A researcher may **apply** to a REC for approval of a research proposal. The REC will **receive and review** research proposals. The REC will **notify** the researcher of its decision and may require additional conditions to protect people's privacy and safeguard their personal health information.
4. Once the researcher has received approval from the REC, the researcher may request the custodian to **disclose** personal health information.
5. The health information custodian **may**, but does not have to, decide to share patient information with the researcher.
6. The custodian and researcher must have a **signed research agreement**.
7. If a REC requires the patient's **express consent**, a custodian can contact patients to see if they want to provide express consent to having their personal health information shared with the researcher.
8. The custodian can charge the researcher **fees** for the costs of providing disclosure.
9. A researcher must follow any **conditions** set by a REC and the custodian.
10. All **disclosures** must be recorded.



(See [Processing Research Requests at-a-Glance](#) in the Resources of the HIA Guide)

8 Information Managers and Information Management Agreements

Introduction

A health information custodian may require assistance with some specific services such as information technology (IT), information systems (IS), or information management (IM). A person or organization that offers one or more of those services may become an **information manager** of the custodian. Under the *Health Information Act* (HIA) an information manager is also considered an agent.

Before using the services, a custodian and an information manager are required to sign an **information management agreement**. A custodian relies on signed information management agreements when authorizing access to personal health information by health information managers.

This chapter includes the following **key concepts**:

1. Responsibilities of the information manager
2. Information management agreement requirements

What is an Information Manager?

An information manager is a person or organization that provides IT, IS or IM services for a custodian or manages personal health information on behalf of a custodian. For example, the GNWT Technology Service Centre (TSC) and the Yellowknife Health and Social Services Authority are information managers.

Other examples of information managers are contracted transcription services and remote backup and off-site records management and retrieval services. A custodian may have more than one information manager.

(See HIA s.13(7), *Certainty*)

Examples

William is a computer technician who owns a company that provides computer technical support to private physicians. When he provides technical support to a physician, he is an **information manager**.

Yellowknife Health and Social Services Authority provides IT, IS, and IM services that support the Territorial EMR system on behalf of other HSSAs and DHSS (other custodians). YHSSA is an **information manager** because they are the lead agency responsible for the EMR, which other HSSAs contribute to.

A custodian does not require additional consent from the patient before sharing their information with the information manager. The custodian assumes the responsibility for making sure that the information manager meets all of the safeguards. The custodian can reassure patients, if required, that their information continues to be maintained in a private and confidential way even when an

outside business or organization has access to it. When a custodian hires an information manager, the custodian continues to be responsible for the privacy and security of the patient's health information.

Responsibilities of the Information Manager

The information manager must collect, use, and disclose patient health information that is provided by the information custodian only for the purposes identified in the information manager agreement.

As agents under the HIA, information managers must comply with the Act. Information managers who do not follow the HIA and their agreement with a custodian can be charged under the HIA.

Information Management Agreement Requirements

A custodian and information manager must sign an **information management agreement (IMA)** before the information manager can begin working. The custodian can only share information with the information manager according to the agreement.

(See HIA s.13(2),(4),(5),(8))

An IMA:

- identifies the standards, policies, procedures, and safeguards information managers and their employees will follow to protect personal health information;
- requires the information manager to comply with the HIA and its Regulations;
- requires the information manager to maintain administrative, technical, and physical safeguards for the protection of personal health information.

When the health information custodian is the DHSS or an HSSA, an IMA is not required if:

- The information manager is an employee of the DHSS or an HSSA.
- The information manager is the DHSS or an HSSA.
- The DHSS has already entered into an IMA on behalf of one or more HSSAs and the DHSS.

When the health information custodian is a physician or pharmacist in the private sector, an IMA is not required if:

- The information manager is an employee of the physician or pharmacist.
- The DHSS has already entered into an IMA on behalf of the physician or pharmacist.

Examples

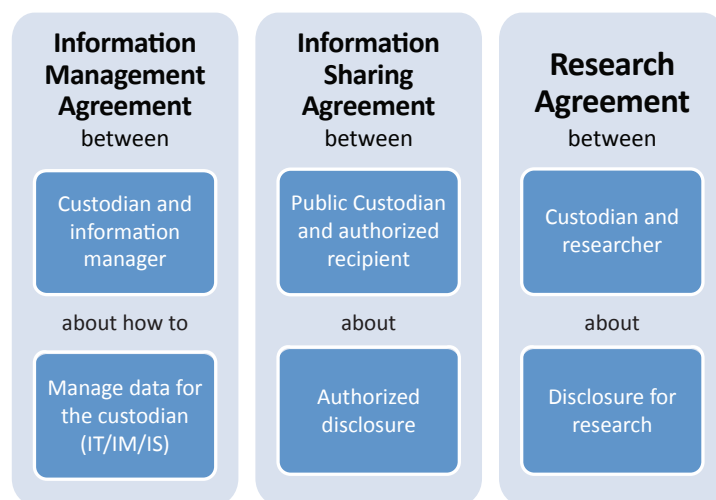
The Yellowknife Health and Social Services Authority is acting as the information manager for the Territorial EMR system on behalf of DHSS and HSSAs, so an IMA is not necessary for YHSSA to provide information management services for the other HSSAs.

If DHSS signs an IMA with the Government of Alberta for a shared interoperable Electronic Health Record (iEHR) system and gives private pharmacists access to this system, an additional IMA would not have to be signed between private pharmacists and the Government of Alberta.

Comparison

Information management agreements (IMA), information sharing agreements (ISA), and research agreements (RA) all require the custodian to authorize access to patients' personal health information. Figure 1 compares these agreements.

Figure 1. Comparison of Information Manager Agreements, Information Sharing Agreements, and Research Agreements



Examples of information sharing initiatives include the territory-wide e-health information systems, Canadian Institute for Health Information, and NWT Bureau of Statistics for health system planning purposes.

(See HIA s.61, *Disclosure to prescribed person or organization.*)

Resources

These resources and templates are available at the end of the Health Information Act Guide. Click on the hyperlink or use the bookmarks to view them.

[Comparison of Information Management Agreements, Information Sharing Agreements, and Research Agreements](#)

Information management agreements (IMA), information sharing agreements (ISA), and research agreements (RA) all require the custodian to authorize access to patients' personal health information.

Chapter 8. Information Managers and Information Management Agreements – Test Your Knowledge

The following quiz applies many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 177](#).

1. Which of the following is an agreement between a custodian and a business or organization to store patients' medical records remotely?
 - a. information management agreement
 - b. information sharing agreement
 - c. research agreement
2. A written agreement between a custodian and a business or organization must be in place before the custodian can share the information.
 - a. true
 - b. false
3. In general, an Information Management Agreement is required when:
 - a. sharing patient health information to another custodian for the continuing care and treatment of the patient
 - b. a custodian agrees to participate in a research study
 - c. non-identifiable data is provided to a third party
 - d. none of the above, an IMA is required for IM/IT/IS services

Chapter 8. Information Managers and Information Management Agreements – Summary of Key Concepts

1. An **information manager** is a person or organization that provides information technology, information systems, or information management (IT/IS/IM) services for a custodian or manages personal health information on behalf of a custodian.
2. The custodian **does not require additional patient consent** before sharing the patient's health information with the information manager.
3. The custodian **assumes the responsibility** for ensuring that the information manager meets all of the safeguards.
4. A custodian and information manager must sign an **information management agreement (IMA)** before the information manager can begin working (some exceptions apply).
5. An **IMA**
 - identifies the standards, policies, procedures, and safeguards that information managers and their employees will follow to protect personal health information;
 - requires the information manager to comply with the HIA and its regulations;
 - requires the information manager to maintain administrative, technical, and physical safeguards for the protection of the personal health information.
6. The information manager will collect, use, and disclose patient health information that is provided by the information custodian **only for the purposes identified** in the IMA.

9 Information and Privacy Commissioner

Introduction

This chapter discusses the powers and responsibilities of the Information and Privacy Commissioner (IPC). The IPC plays an important privacy oversight role.

This chapter includes the following **key concepts**:

1. IPC appointment and role
2. IPC powers and duties

IPC Appointment and Role

The IPC for the *Health Information Act* (HIA) is appointed under the *Access to Information and Protection of Privacy Act* (ATIPP). This means that the IPC provides oversight for both ATIPP and the HIA. A Special IPC can be appointed to act on a specific matter related to the HIA. The Special IPC holds her or his office until that matter is resolved.

The IPC takes an oath specific to the HIA to act impartially and not disclose any information received by the Office of the IPC unless disclosure is allowed by the HIA. The IPC may have staff who must also take an HIA oath.

The IPC may delegate powers and duties to staff, except the power to:

- delegate
- establish rules for reviews
- allow an alternative means of providing a required notice
- allow notice to be given to someone on behalf of the person who should get the notice
- perform a prescribed duty or function

A delegation must be in writing and can contain conditions.

(See HIA s.169-172, IPC.)

IPC Powers and Duties

The IPC is responsible for promoting compliance with the HIA and for ensuring custodians properly protect patient information and their privacy. The IPC is available to help health information custodians and patients find solutions to privacy issues.

The IPC is independent from government and has the power to review the conduct of health information custodians. The IPC has recommendation-making powers under the HIA.

The IPC's general powers and duties include:

- informing the public about the HIA
- receiving comments about the HIA
- participating in research that affects the purpose of the HIA (to protect patient privacy and allow easy flow of information in the health system)
- providing advice to custodians
- commenting on how proposed legislation, programs, and services may affect patients' privacy and access to personal health information

(See HIA s. 174, *General powers.*)

The IPC can comment on privacy impact assessments (PIAs) done by custodians.

(See HIA s.175, *Privacy impact assessments.*)

A public register of reports and recommendations of the IPC helps custodians to understand and interpret the HIA. The IPC must keep a public register of reports and recommendations made under the HIA. Before entering a report or recommendation in the public register, the IPC must conceal the identity of any person whose personal health information is included.

(See HIA s.177, *Duty to maintain register.*)

The IPC can share information that relates to an offence with law enforcement if necessary.

(See HIA s.178(5), *Disclosure relating to offence.*)

Annual Report

By October 31 each year, the IPC must submit an HIA report to the Legislative Assembly. The report must include:

- an assessment of the effectiveness of the HIA
- a report on the activities of the IPC under the HIA during the previous year
- information about situations when the IPC's recommendations after a review were not followed
- recommendations or comments on matters relating to the HIA

(HIA s.173, Annual report.)

Procedure and Evidence on Review

The IPC will create the procedures and evidence rules that will be followed when the IPC reviews access and correction requests or privacy complaints from individuals.



(See [Chapter 10, Access to and Correction of Personal Health Information](#) and [Chapter 12, Privacy Breach](#).)

The IPC can make rules about reviews and alternative dispute resolutions done under the HIA.

(See HIA s.148, Rules.)

Custodians must produce any records the IPC needs. These must be produced within 14 days. The IPC can view records (for example, on electronic health information systems) if copies cannot be produced within 14 days. The IPC can require any evidence to be submitted and does not have to stick to the rules of court. No one can withhold evidence from the IPC.

(See HIA s.152, Evidence.)

Evidence collected by the IPC cannot be used in court, with the following exceptions:

- perjury cases
- cases in which someone is charged under the HIA
- appeals made to court in accordance with the HIA

(See HIA s.154, Additional powers of IPC and evidence.)

Evidence collected during an alternative dispute resolution cannot be used in court without the consent of everyone involved.

(See HIA s.155, Evidence from alternative dispute resolution process.)

The Supreme Court cannot require the IPC to give evidence in court unless the matter concerns a review started by the IPC.

(See HIA s.179, Non-compellability; s.161, Appeal by IPC of decision by custodian.)

During a review, the IPC:

- can ask anyone to attend as a witness
- may require anyone to give evidence under oath or affirmation
- has the same powers as a civil court

Resources

These resources and templates are available at the end of the Health Information Act Guide. Click on the hyperlink or use the bookmarks to view them.



(For more information about the IPC, see [Chapter 10, Access to and Correction of Personal Health Information](#) and [Chapter 11, Privacy Breach](#).)

Chapter 9. Information and Privacy Commissioner – Test Your Knowledge

The following quiz applies to many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 177](#).

1. IPC stands for:
 - a. Information and Privacy Commissioner
 - b. Intellectual and Privacy Committee
 - c. Information and Privacy Company
2. The IPC is appointed under what act?
 - a. Legislative Assembly Act
 - b. Access to Information and Protection of Privacy Act (ATIPP)
 - c. Health Information Act (HIA)
3. The IPC may collect evidence during a review or appeal. The information can be used:
 - a. in the course of a review
 - b. in her report
 - c. for law enforcement purposes (relating to an offense)
 - d. for prosecution, application or appeal
 - e. all of the above
4. The IPC plays what role under the HIA?
 - a. An information manger
 - b. Custodian
 - c. An oversight role

Chapter 9. Information and Privacy Commissioner – Summary of Key Concepts

1. The IPC is **appointed** under the *Access to Information and Protection of Privacy Act* (ATIPP).
2. The IPC is **independent** from government and has the power to review the conduct of health information custodians.
3. The IPC provides **oversight** for the HIA.
4. The IPC is responsible for **promoting compliance** with the HIA and for ensuring custodians properly protect patients' personal health information and their privacy.
5. The IPC's general **powers and duties** include:
 - informing the public about the HIA
 - receiving comments about the HIA
 - participating in research that affects the purpose of the HIA (to protect patient privacy and allow easy flow of information in the health system)
 - providing advice to custodians
 - commenting on how proposed legislation, programs, and services may affect patients' privacy and access to personal health information
6. The IPC can **comment** on privacy impact assessments (PIA) done by custodians.
7. The **public register** of reports and decisions of the IPC helps custodians to understand and interpret the HIA.

10 Access to and Correction of Personal Health Information

Introduction

People have a right to access their health information in the custody or under the control of a custodian.

In 1992 the Supreme Court of Canada (McInerney v. MacDonald) ruled patients have the right to examine and get a copy of the information in their medical records. The *Health Information Act* (HIA) ensures patients' right to access, view, and correct their personal health information.

This chapter includes the following **key concepts**:

1. Patients' right to access their own records
2. Exceptions to the right to access
3. Patients' right to correct their own records
4. Access and correction request processes
5. Review and appeal process

Patients' Right to Access Their Own Records

A patient has the right to access their personal health information in the custody or under the control of a custodian. This includes information that is documented in:

- hard copy,
- electronic copy, or
- any other media format, including audio recording, text, digital photography, and
- any other new and emerging technologies that may be used to store health information.

The patient's substitute decision-maker also has a right to access the information.



(For more information on substitute decision makers, see [Chapter 3, Consent](#).)

However, a patient's right of access does not extend to information that would be exempted from disclosure.

(See HIA s.110-118, *Exceptions to providing access*.)

Patients can obtain copies of their health records, but not the original documents. The applicant may ask for a copy of the record or ask to examine the record. The applicant can ask for a hard copy or an electronic copy.

If a record is not in the custodian's hands, but the custodian has the power to retrieve it, then the record is in the custodian's control. You may have sent a file to storage, but if you can retrieve it, the record is still in your control. In the event that a custodian may have control but not custody of an electronic record, the custodian is still responsible for handling access requests. A custodian that uses the NWT Electronic Medical Record (EMR) system must respond to access requests as if the patient information on the system is in their custody.

If a patient requests from a custodian a record of who has viewed or added to the patients' health information, referred to as record of activity, the custodian must process this request as an access request.

(See HIA s.84, *Requirement to maintain disclosure information*.)

On occasion, a patient may make an access request that is trivial or in bad faith. The custodian can ask the Information and Privacy Commissioner (IPC) for permission to disregard the request.

Informal Disclosure and Formal Access Request

A health service provider may provide access to a patient's personal health information using **informal disclosure** by sharing the patient's personal health information with the patient during a medical appointment or consultation. In this case, patients do not need an access request form to receive their own information. A verbal request is sufficient.

Table 1. Informal Disclosure and Formal Access Requests

Informal Disclosure to Patient	Formal Access Request
A patient asks for a copy of today's clinic note. She receives a photocopy of the record. The clerk writes a disclosure notation on the patient record.	A former residential school student asks for a copy of her medical record. The access request is in writing. The custodian follows the formal access procedure.
Parents of a baby attend the immunization clinic at Public Health. The parents bring the immunization booklet for the child, and the nurse updates the record with today's immunization information.	A patient requests that a copy of his medical records for the last specialist consultation appointment be mailed to his home. The access request is in writing. The custodian follows the formal access procedure.
Summary: The request usually occurs on the day when the health service is provided. The patient receives the disclosure the same day.	Summary: The written request usually is received after the health service is provided. The disclosure is processed as soon as possible (days) after the request is made.

(See HIA s.90, Definition "applicant"; s.91, Disclosure without formal request.)

Exceptions to the Right of Access

The HIA gives patients the right to access their personal health information. However, the HIA sets out certain circumstances when the custodian either may not or must not give access.

Mandatory Exceptions

A custodian must not give a patient access to information that would be an invasion of someone else's privacy. However, if the patient him- or herself provided information about someone else, the patient can get access to that information.

(See HIA s.110, Invasion of privacy.)

Patients do not have a right of access to records created during a Quality Assurance Committee activity. However, information compiled for the committee's records may have been copied from patients' medical records. If this is the case, a patient still has the right to access information from his or her original record.

Custodians may share results and recommendations of a quality assurance activity or review.

(See HIA s.111(2), Quality assurance activity.)

A custodian cannot disclose information to a patient if the disclosure is prohibited by law.

(See HIA s.112, Disclosure prohibited by Act.)

A public custodian cannot disclose records that would reveal confidential information presented to the Executive Council or the Financial Management Board.

(See HIA s.117, Executive.)

Discretionary Exceptions

A custodian may refuse to disclose a patient's personal health information to the patient if a medical or mental health professional believes this could cause an imminent threat or risk of serious harm to the health or safety of the patient.

(See HIA s.113(1), Disclosure harmful to applicant.)

Custodians can refuse to share information with a patient if this could result in an imminent threat or risk of serious harm to the health or safety of anyone, or a threat to public safety. These requests may include situations where the information was provided to the health care provider by another party in confidence and subsequently added to a patient's health care record.

(See HIA s.113(2), Disclosure harmful to individual or public safety.)

A custodian may refuse to disclose information to a patient if it identifies another person who gave information about the patient to the custodian in confidence and it is best to keep that person's identity secret.

Example

David's wife Joy tells their doctor that David is driving even though he has fainting spells. She asks the doctor not to let David know she "told on him" because David "has a terrible temper."

After talking with Joy, the doctor refers David for an electrocardiogram (ECG) when he has his annual check-up. Based on the results, the doctor tells David he must stop driving. If David requests a copy of his health record, the information from Joy should be severed for her own protection.

(See HIA s.114, Information provided in confidence.)

A custodian may refuse to share information with a patient if the information is "privileged." Legal advice to a custodian or agent is an example of privileged information.

(See HIA s.115, Privilege.)

A custodian may refuse to disclose information to an applicant if the disclosure could do any of the following things:

- interfere with law enforcement
- reveal the identity of a confidential source
- reveal a record that has been confiscated from a person by a peace officer in accordance with a law

(See HIA s.116, Law enforcement matter.)

A public custodian may refuse to disclose information if the disclosure could reveal internal and health system management advice and analysis, or advice by or for a Minister, or consultations with a Minister or Minister's Office.

(See HIA s.118, Disclosure of advice from officials.)



(See ["Access Requests at-a-Glance"](#) in the Resources section of the HIA Guide for a summary of mandatory and discretionary exceptions under the HIA.)

Access Request Process

Getting Started

Custodians have a responsibility to help patients prepare access applications. This is called a "duty to assist."

Patients may want personal health information for their own use, or they may ask to have their records transferred to a different health service provider. A patient who asks for a copy of her or his own health record completes an access request form. The office then retrieves, reviews, and processes the records.

(See HIA s.97, Duty to assist applicant.)

When patients make access requests, custodians must make every reasonable effort to respond accurately.

Ask patients:

- “What information do you want?”
- “Why do you want it? We can help you to locate the most appropriate information that best meets your needs.”

If the request is too broad, try to narrow the request to the least amount of information that meets the applicant’s needs.

- “Where do you want us to send it?”

Make sure you are sending the correct information to the right place. Custodians and their agents must make a reasonable effort to ensure that personal health information is disclosed to the person who is authorized to receive it. Ask to see at least two patient identifiers before providing records for a patient. The custodian must follow required measures to safeguard the information accessed.

(See HIA s.93, Duty of custodian: identity of applicant.)

The access request must include enough detail to enable the health information custodian to identify the record. If needed, the custodian must ask for additional information to process the access request. The custodian must contact the patient within 10 days of receiving the access request.

Custodians must share information with patients as quickly as possible and within 30 days.

(See HIA s.103(2), Duty to provide access within 30 days.)

Within 30 days of receiving an access request, a custodian may ask the IPC for permission to disregard a patient’s access request. *(See HIA s.105, s.129 for details.)*

A custodian who asks the IPC for such permission must give notice to the patient.

The IPC must review the request and make a decision in writing. The IPC can allow a custodian to ignore a request for the following reasons:

- The request is frivolous or vexatious.
- It is made in bad faith.
- It concerns a trivial matter.
- It amounts to an abuse of the right of access.
- Giving the patient access to his or her health record would unreasonably interfere with the custodian’s work because it is repetitive or systematic.

Copies of the IPC decision go to the custodian and patient.

This decision cannot be appealed.

(See HIA s.130, Review of request; s.129, Request for authorization to disregard access request; s.131, Authorization to disregard access request.)



(See “[Access to Personal Health Information Process](#)” in the Resources section of the HIA Guide for a flowchart of the access process under the HIA.)

Transferring an Access Request

A custodian may transfer an access request or part of a request to another custodian if some or all of the applicant’s health record:

- was made by the other custodian
- was first collected by the other custodian
- is in the custody of the other custodian

The custodian must notify the patient right away when a request is transferred. The notice will state:

- that the access request has been transferred
- the reason for the transfer
- the health information custodian to which the access request has been transferred
- the patient's right to ask the IPC to review the transfer

The custodian receiving the transfer must give the patient the designated contact person's contact information.

(See HIA s.108, Transfer of access request.)

If a custodian accepts the transfer of an access request, the clock starts at the beginning once the request is transferred. The receiving custodian must follow the same timeframes set out previously in the HIA.

(See HIA s.109, Duties of receiving custodian.)

Fees

Fees can be charged for access requests, but the fees cannot exceed the costs to the custodian. See the *Health Information Regulations* for the Fee Schedule. Private and public custodians may waive payment.

Custodians may charge specified fees to process access requests. However, any fee requirement cannot be a barrier to a patient's ability to access his or her own information. When determining a fee, a custodian should consider the overall purposes of the HIA, which include giving people the right to their personal health information. If a fee estimate is high or a patient objects to it, the custodian has a duty to assist the patient determine if less information could be requested. The fee could be lowered or waived.

Example

Norman is planning a holiday. He phones the health centre to ask for a copy of his medical record to take with him. The receptionist asks Norman to come to the health centre to fill out an access request form. She tells Norman that a fee might be charged.

Norman is upset. He has limited finances at the moment and does not think he should have to pay to get his own information. The receptionist refers him to the designated contact person. She explains that the fee is charged for processing his request, however if the fee is a hardship for Norman and will stop him asking for a copy of his information, the fee can be waived. The designated contact person prepares a cost estimate for Norman. He reviews the fee estimate and confirms he cannot afford the fee. The health centre waives the fee and processes the access request.

The estimate of fees and disbursements must include all applicable fees set out in Part 1 of Schedule B of the Regulations. There is no fee for the following:

- access of personal health information through a patient portal
- if the information is held by a public custodian, examination of personal health information at a health facility during regular business hours.

Fees may only be charged if the estimate is greater than the base amount set out in the Regulations.

(See Health Information Regulations s.9.)

The **fee estimate must occur within 20 days** of receiving the request (or within 20 days of receiving all the information needed to process the request).

(See HIA s.104(2), Estimate of fees.)

When applicable, **the patient will be invoiced within 10 days after he or she agrees to the fee estimate.** The amount of an invoice must not be more than the fee estimate and the actual cost of providing access. The custodian provides access (copy or view of the patient's personal health information) only after the invoice is paid.

(See HIA s.104, Further information required, fee estimate, invoice, time limit; Health Information Regulations s.9–11.)

Timelines

Custodians must process access requests as soon as possible. When a patient applies for access to health records, the custodian must reply in writing within 30 days. The 30-day time limit does not apply if:

- More information is required.
- The request has been transferred to another custodian.
- A custodian has asked the IPC to allow it to disregard the request and the IPC has allowed the custodian to disregard it.
- There is a time extension.
- The applicant has abandoned the request.
- The applicant has not provided confirmation to proceed after a fee estimate.
- An IPC review of the request is done during the initial 30-day limit.

If the custodian needs more information from the patient in order to process her or his access request, the custodian must **ask the patient for more information within 10 days** after getting the request. The custodian cannot wait until day 30 and then use the missing information as an excuse to delay responding. The custodian must tell the patient that he or she must respond within 60 days or the custodian may close the request. If a patient does not reply to a custodian's request for more information, the custodian can close the request 60 days later. Closing a request does not stop a patient from making the same access request again.

(See HIA s.104(1), Further information required.)

If a custodian **transfers an access request** or part of a request to another custodian, the custodian that accepts the transfer of an access request must follow the timelines starting once the request is transferred.

If the custodian asks the IPC to review a request to determine if the custodian can **disregard** the request, the **clock stops**. If the IPC denies the custodian's request, the **clock starts** on the day the custodian receives notice of the IPC's decision, with any delays or extensions otherwise allowed.

(See HIA s.129, Request for review to disregard an access request; s.130, Review of request; s.131, Authorization to disregard access request.)

If the custodian requires more time to respond to the access request, the custodian can **extend the 30-day time limit** by no more than another 30 days. The time limit may be extended if:

- A large number of records must be reviewed.
- The custodian needs to consult with someone to make sure the applicant has a right to the record.

A health information custodian that extends the time limit must tell the applicant:

- that the time limit is extended
- the reason for the extension
- when the patient will be told whether or not his or her request is approved
- that the patient can ask the IPC to review the time extension

The custodian must respond to the patient before the extension ends. If the custodian anticipates that it will require additional days, the custodian must apply to the IPC for an extension. The custodian should **apply to the IPC for an extension** at the same time that the health information custodian issues its 30-day extension.

If the IPC denies the extension, the custodian must respond to the patient within 30 days of receiving the IPC's decision.

(See HIA s.106, *Extension of time limit for responding*; s.132, *Request for extension of time limit: access request*; s.133, *Review of request*.)



(See [“Access Request Timelines”](#) in the Resources section of the HIA Guide for a summary of timelines for access requests under the HIA.)



To assist custodians when responding to an access request, see [“Formal Access Request: Suggested Tasks and Timelines”](#) in the Resources section of the HIA Guide.

Custodians may use this as a worksheet for more complicated access request to record start and stop dates in the access timelines. The worksheet summarizes key steps required to process access requests. These steps are referenced below.

Response

In responding to an access request, the custodian may decide to grant access or not. The custodian must prepare a response. If access or partial access is **granted**, the custodian must tell the patient when and how to access the record. If access is **denied**, the custodian must explain why and inform the patient he or she can complain to the designated contact person or ask the IPC to review the decision.

After the custodian responds to the patient that access or partial access is granted, the custodian has up to another 30 days to provide the records to the patient if access to the records does not occur at the time of the response.

If a patient asks for a copy of her or his record and the custodian determines she or he is entitled to the information, the custodian must provide a copy unless the record cannot be copied. If that is the case, the custodian must allow the patient to see the record or have access in another way. (For example, an interactive system called a “patient portal”

could be developed to give patients access to their information.)

If a patient asks to see his or her record and the custodian has determined the patient is entitled to the information, the custodian must allow the patient to examine the record. If letting the patient see the record could lead to a security risk, the patient must be given a copy with any prohibited information severed.

If there is a security risk to real property or to an electronic health information system or communications system, the custodian can refuse to let the patient see the information in the building or on the system.

(See HIA s.99, *Request for copy of record*; s.100, *Prejudice to security*.)

Patient Request for IPC Review of Access Request

A patient who makes an access request to a custodian may ask the IPC to review any decision or action of a custodian that is related to the request.

A request for review must be made in writing to the IPC. The review should be requested within 60 days after the issue occurred or within 60 days after the patient became aware of the issue. A patient who does not get a response from a custodian on time can assume the custodian is refusing access.

Example

Mary is moving to a different community. She asked her doctor for a summary of her personal medical record. Mary filled out the request form at the health centre over a month ago. She has not received any information from the health centre.

Mary asks the IPC to review her access request.

The IPC **must** give copies of the request for review to the custodian and may give copies to others affected. The IPC may sever information in a request before giving it to a person or organization.

(See HIA s.141, Request for review: access and correction requests; s.142, Requirements and timing.)

The IPC may review any decision, act, or failure to act by a custodian who has been asked to give access to a record by the person who is the subject of the record. The IPC may, without conducting a full review, refuse the request if:

- The request is frivolous.
- It is made in bad faith.
- It concerns a trivial matter.
- The patient is taking unnecessary advantage of the right to a review.
- It concerns a matter that has already been dealt with under the HIA or the ATIPP.

(See HIA s.143 (2), Grounds for refusal, discontinuance.)

After a patient requests a review for an access request, the IPC may, without conducting a full review, assist the patient and the health information custodian to resolve the matter. A formal or informal **alternative dispute resolution process** may be followed to settle the disagreement. Methods include negotiation, conciliation, mediation, and arbitration.

The IPC may authorize a mediator to attempt to settle a dispute. If the matter is resolved, the IPC must make a record of the resolution.

(See HIA s.144, Alternative dispute resolution; s.141(1), Request for review: access request.)

If the dispute is not resolved through alternative dispute resolution, the IPC must prepare a report on any access request review. The report should include the following information:

- whether or not the IPC agrees with the decision of the custodian
- the IPC's reasons for agreeing or disagreeing

The IPC can make a report that includes recommendations to the custodian, whether or not the IPC agrees or disagrees with the custodian's actions. The IPC's report should be completed within 120 days of receiving the request for review.

(See HIA s.146, IPC report; s.149, Time limit for review.)

The IPC must give a copy of the report to the patient, custodian, and Minister. Copies may also be given to anyone else affected by or involved in the review.

(See HIA s.147, Requirement to give copy of report.)

Custodian's Decision on IPC Recommendations

Within 30 days after getting the IPC's recommendations, the custodian must notify the following people whether or not it accepts any or all of the recommendations:

- the IPC
- the person who requested the review
- the Minister of Health and Social Services

A custodian who decides not to accept one or more of the IPC's recommendations must tell the person who requested the review that he or she has the right to appeal the custodian's decision to the NWT Supreme Court.

If the custodian does not respond within 30 days, everyone must assume the custodian does not accept the recommendations. The IPC can share the custodian's response with anyone involved in the review. A custodian who accepts any IPC recommendation must follow it within 45 days of responding.

(See HIA s.156, Custodian's decision: IPC recommendations; s.157, Notice of decision; s.158, Requirement to comply with decision.)

Appeal to Supreme Court

Patients have the **right to appeal** a custodian's decision to the Supreme Court. A patient who requested any type of review can appeal to the Supreme Court any decision the custodian makes in response to the IPC's recommendations. An appeal to the Supreme Court must be made within 30 days after the patient receives the custodian's decision as to whether or not it accepts the IPC's recommendations. If the custodian does not respond to the IPC's recommendations, the patient has 90 days to appeal to the Supreme Court.

(See HIA s.160, Appeal by individual of decision by custodian.)

The IPC's recommendations cannot be appealed. If the patient believes the IPC based recommendations on an incorrect assumption made during a review of the evidence gathered, then the patient can appeal that assumption/finding of the IPC's. The appeal must be made to the Supreme Court within 30 days of getting the IPC's report.

(See HIA s.159(2), Appeal by individual of IPC finding: access request, correction request.)

If the IPC started a review of a custodian's activities, and the custodian decides not to accept any or all of the IPC's recommendations, the IPC may appeal to the Supreme Court. The appeal must be filed within 30 days after the IPC gets the custodian's decision. If the custodian does not respond to the IPC's recommendations, the IPC has 90 days to appeal to the Supreme Court.

The IPC is not a party in a Supreme Court appeal case unless the IPC started the review.

(See HIA s.161, Appeal by IPC of decision by custodian.)

On an appeal, the Supreme Court shall make its own determination of the matter. The Supreme Court can examine any record held by the custodian. No one can withhold evidence. The Supreme Court can share information with law enforcement if it thinks a crime has been committed.

(See HIA s.165, Disclosure of information relating to offence.)

If a custodian says a patient has no right to access the record requested, the custodian must prove this to the Supreme Court.

(See HIA s.166, Onus: appeal relating to access request.)

The Supreme Court can make any order and set any conditions it considers appropriate. An order of the Supreme Court is final and cannot be further appealed apart from a review of court process during the appeal. A person or organization shall comply with an order within the time set in the order, or if no time is set, within 45 days after the order is issued.

(See HIA s.167, Order of Supreme Court.)

Patients' Right to Have Their Information Corrected

We all have a responsibility to make sure every patient's personal health information is accurate and complete.

Patients can ask to have information in their medical records corrected if they think it has an error or omission. Custodians must assist patients with their correction requests and must respond openly and accurately without delays.

No fees can be charged for corrections.

Nothing stops a health service provider from correcting a patient's medical record if the patient requests the change during an appointment or consultation.

Example

When Martha checks in at the health centre, she notices that the health centre does not have her updated street address. The clerk compares the information that Martha provides from her driver's license with the information in her current record. The clerk updates the health centre's record for Martha.

(See HIA s.92, Correction without written request.)

Correction Request Process

Getting Started

Health information custodians have a responsibility to help patients prepare correction requests. This is called a "duty to assist."

(See HIA s.119, Correction request.)

When patients make correction requests, custodians must make every reasonable effort to respond accurately and quickly. If the request is too broad, try to narrow the request to the most specific information that the applicant is concerned about.

Ask patients:

- "Exactly what information do you want changed?"

Make sure you are correcting information in the correct record. Ask to see at least two patient identifiers before confirming the record to be changed. The custodian must follow required measures to safeguard the correction process.

The correction request must include enough detail to enable the health information custodian to identify the record. If needed, the custodian must ask for additional information to process the correction request. The custodian must contact the patient within 10 days of receiving the correction request.



(See "[Correction to Personal Health Information Process](#)" in the Resources section of the HIA Guide for a flowchart of the correction process under the HIA.)

Timelines

Custodians must process correction requests as soon as possible. Within 30 days of getting the correction request, custodians must either:

- make the correction and tell the patient in writing; or
- tell the patient in writing that they will not make the correction.

The 30-day time limit does not apply if there is a **time extension**.

Within 10 days of getting the request, the custodian must **ask the patient for more information**, if this is necessary. The custodian cannot wait until day 30 in order to delay responding. If more information is required to make a decision, the custodian must respond to the request 30 days after getting the additional information. The custodian must tell the

patient that he or she must respond within 60 days or the custodian may close the request. If a patient does not reply to a custodian's request for more information, the custodian can close the request 60 days later. Closing a request does not stop a patient from making the same correction request again.

(See HIA s.122, Further information required.)

The custodian can **extend the 30-day time limit** by no more than another 30 days if:

- Many records must be reviewed.
- The custodian needs more time to consult with someone to see if the correction request should be denied.

A custodian that extends the time limit must give the applicant the following information as soon as possible:

- the extension of the time limit
- the reason for the extension
- the date by which the response required will be given (under subsection 101(1))
- that the applicant may ask the IPC to review the time extension (under subsection 141(2))

The custodian must respond to the patient before the extension ends. If the custodian anticipates that it will require additional days, the custodian must apply to the IPC for an extension. The custodian should **apply to the IPC for an extension** at the same time that the health information custodian issues its 30-day extension. If the IPC denies the extension, the custodian must respond to the patient within 30 days of receiving the IPC's decision.

(See HIA s.123, Extension of time limit for compliance; s.124, Suspension of time limit if review by IPC; s.132, Request for extension of time limit: access request; s.133, Review of request.)



(See "[Correction Request Timelines](#)" in the Resources section of the HIA Guide for a summary of timelines for correction requests under the HIA.)

Response

The custodian must make a decision to make the correction or refuse the correction.

A custodian that makes a correction must make a reasonable effort to give the corrected information to anyone it shared the original record with in the past year. If the patient states in writing that this is not necessary, the custodian does not have to inform others of the correction. If the custodian believes that no harm will come to the patient, it also does not have to share the corrected information. If a patient specifically requests that others be informed of the correction, the custodian must, no matter what, inform everyone it shared the record with in the past year.

The custodian must make the correction right away after the decision to grant the correction is made. No delay is allowed.

Any custodian that receives notice of a correction must change its record.

(See HIA s.128, Duty to forward correction.)

A custodian may refuse to make a requested correction for the following reasons:

- The patient has not proved there is an error.
- The information is a professional opinion made in good faith.
- The record was not made by the custodian and the custodian is not an expert in that field and so cannot know if the correction makes sense.
- The request is frivolous or made in bad faith.

(See HIA s.125, Grounds for refusal.)

If the correction request is refused, the custodian's response to the patient must include the following information:

- the reason for the refusal
- how to get in touch with the designated contact person if the patient has questions
- that the patient may ask the IPC for a review

- that the patient may provide a statement of disagreement, giving her or his reasons for disagreeing with the custodian's refusal

If the custodian refuses to make a correction in the patient's record, the patient can take any or all of the following actions:

- Ask the custodian to attach the correction request to the record.
- Ask the IPC for a review.
- Make a formal statement of disagreement.

A custodian that receives a statement of disagreement must attach the statement to the medical record or include a cross-reference to the statement. The patient may request the custodian also attach the correction request to her or his medical record.

The custodian must also make a reasonable effort to provide a copy of the statement of disagreement or the correction request to anyone it has shared the record with in the past year.

A receiving custodian must also attach the statement of disagreement or the correction request to its copy of the record.

(See HIA s.126, Statement of disagreement; s. 127, Duty of custodian: statement of disagreement.)

Patient Request for IPC Review of Correction Request

A patient who makes a correction request to a custodian may ask the IPC to review any decision or action of a custodian that is related to the request.

A request for review must be made in writing to the IPC. The review should be requested within 60 days after the issue occurred or within 60 days after the patient became aware of the issue. A patient who does not get a response from a custodian on time can assume the custodian is refusing the correction request. At this point, the patient can ask the IPC for a review.

(See HIA s. 121, Deemed refusal; s.141(2), Request for review: correction request.)

The IPC **must** give copies of the request for review to the custodian and may give copies to others affected. The IPC may sever information in a request before giving it to a person or organization.

(See HIA s.141, Request for review: access and correction requests; s.142, Requirements and timing.)

The IPC may review any decision, act, or failure to act by a custodian who has been asked to correct or amend a record by the person who is the subject of the record. The IPC may, without conducting a full review, refuse the request if:

- The request is frivolous.
- It is made in bad faith.
- It concerns a trivial matter.
- The patient is taking unnecessary advantage of the right to a review.
- It concerns a matter that has already been dealt with under the HIA or the ATIPP.

(See HIA s.143, Review by IPC.)

After a patient requests a review for a correction request, the IPC may, without conducting a full review, assist the patient and the health information custodian to resolve the matter. A formal or informal **alternative dispute resolution process** may be followed to settle the disagreement. Methods include negotiation, conciliation, mediation, and arbitration.

The IPC may authorize a mediator to attempt to settle a dispute. If the matter is resolved, the IPC must make a record of the resolution.

(See HIA s.144, Alternative dispute resolution; s.141(2), Request for review: correction request.)

If the dispute is not resolved through alternative dispute resolution, the IPC must prepare a report on any correction request review. The report should include the following information:

- whether or not the IPC agrees with the decision of the health information custodian
- the IPC's reasons for agreeing or disagreeing

The IPC can make a report that includes recommendations to the custodian, whether or not the IPC agrees or disagrees with the custodian's actions. The IPC's report should be completed within 120 days of receiving the request for review.

(See HIA s.146, IPC report; s.149, Time limit for review.)

The IPC must give a copy of the report to the patient, custodian, and Minister of Health and Social Services (HSS). Copies may also be given to anyone else affected by or involved in the review.

(See HIA s.147, Requirement to give copy of report.)

Custodian's Decision on IPC Recommendations

Within 30 days after getting the IPC's recommendations, the custodian must tell the following people whether or not she or he accepts these recommendations:

- the IPC.
- the person who requested the review
- the Minister

A custodian who decides not to accept one or more of the IPC's recommendations must tell the person who requested the review that he or she has the right to appeal the custodian's decision to the NWT Supreme Court.

If the custodian does not respond within 30 days, everyone must assume the custodian does not accept the recommendations. The IPC can share the custodian's response with anyone involved in the review. A custodian who accepts any IPC recommendation must follow it within 45 days of responding.

(See HIA s.156, Custodian's decision: IPC recommendations; s.157, Notice of decision; s.158, Requirement to comply with decision.)

Appeal to Supreme Court

Patients have the **right to appeal** a custodian's decision to the Supreme Court. A patient who requested any type of review can appeal to the Supreme Court any decision the custodian makes in response to the IPC's recommendations. An appeal to the Supreme Court must be made within 30 days after the patient receives the custodian's decision as to whether or not it accepts the IPC's recommendations. If the custodian does not respond to the IPC's recommendations, the patient has 90 days to appeal to the Supreme Court.

(See HIA s.160, Appeal by individual of decision by custodian.)

The IPC's recommendations cannot be appealed. If the patient believes the IPC based recommendations on an incorrect assumption made during a review of the evidence gathered, then the patient can appeal that assumption/finding of the IPC's. The appeal must be made to the Supreme Court within 30 days of getting the IPC's report.

(See HIA s.159(2), Appeal by individual of IPC finding: access request, correction request.)

If the IPC started a review of a custodian's activities, and the custodian decides not to accept any or all of the IPC's recommendations, the IPC may appeal to the Supreme Court. The appeal must be filed within 30 days after the IPC gets the custodian's decision. If the custodian does not respond to the IPC's recommendations, the IPC has 90 days to appeal to the Supreme Court.

The IPC is not a party in a Supreme Court appeal case unless the IPC started the review.

(See HIA s.161, Appeal by IPC of decision by custodian.)

On an appeal, the Supreme Court shall make its own determination of the matter. The Supreme Court can examine any record held by the custodian. No one can withhold evidence. The Supreme Court can share information with law enforcement if it thinks a crime has been committed.

(See HIA s.165, Disclosure of information relating to offence.)

The Supreme Court can make any order and set any conditions it considers appropriate. An order of the Supreme Court is final and cannot be further appealed apart from a review of court process during the appeal. A person or organization shall comply with an order within the time set in the order, or if no time is set, within 45 days after the order is issued.

(See HIA s.167, Order of Supreme Court.)

Resources

These resources and templates are available at the end of the Health Information Act Guide. Click on the hyperlink or use the bookmarks to view.

[Formal Access Request: Suggested Tasks and Timelines](#)

Use this as a worksheet for more complicated access request to record start and stop dates in the access timelines. The worksheet summarizes key steps required to process access requests under the HIA.

[Access Request Timelines](#)

Summary of timelines for access requests under the HIA.

[Correction Request Timelines](#)

Summary of timelines for correction requests under the HIA.

[Access Requests at-a-Glance](#)

Summary of mandatory and discretionary exceptions under the HIA.

[Flowcharts](#)

Flowchart diagrams to assist you with

1. Access to Personal Health Information Process,
2. Correction to Personal Health Information Process; and
3. Review and Appeal Process under the HIA.

Chapter 10. Access to and Correction of Personal Health Information – Test your Knowledge

The following quiz applies to many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 178](#).

1. A patient has the right to access information that is under the custody or control of the custodian
 - a. true
 - b. false
2. Julia moved recently. On her next visit to the doctor she asks that her address be changed in her medical record. Can she do that?
 - a. Yes
 - b. No
3. A health information custodian has to respond to an access request in writing no later than how many days after receiving the request?
 - a. 14 days
 - b. 60 days
 - c. 30 days
4. George has been diagnosed with schizophrenia. His doctor asked his mother about his behaviour. George's mother responded that her son has been angry, confused, and paranoid for the past six months. After being discharged, George asks to see his medical record. Should he have access to his information?
 - a. Yes. He has the right to all his information.
 - b. No. He should be denied access.
 - c. Yes. He should have access, but the information his mother gave in confidence should be severed first.
5. A custodian may refuse to make a requested correction to a record if
 - a. the request is frivolous or made in bad faith.
 - b. the information is a professional opinion.
 - c. the patient has not proved there is an error in the record.
 - d. all of the above.
6. If a report by the IPC includes recommendations for action by a health information custodian, the custodian can accept the recommendations without taking any additional actions.
 - a. true
 - b. false

Chapter 10. Access to and Correction of Personal Health Information – Summary of Key Concepts

1. Patients have a **right to access** their own records.
2. A health service provider may provide access to a patient's personal health information using **informal disclosure** by sharing the patient's personal health information with the patient during a medical appointment or consultation.
3. When patients make access requests, health information custodians must make every reasonable effort to respond accurately and quickly, generally within **30 days**. Fees can be charged for access requests, but the fees cannot exceed costs to the custodian.
4. Fees can be **waived**.
5. Health information custodians have a responsibility to help patients prepare access and correction applications. This is called a "**duty to assist**."
6. Patients have a **right to have their own records corrected**. Custodians have a **duty to assist** patients with their correction requests and must respond openly and accurately without delays, generally within 30 days. No fees can be charged for corrections.
7. The HIA gives patients the right to their personal health information. However, the **disclosure of patients' information may be limited** by other laws, obligations, or considerations.
8. A health information custodian may refuse to make a requested correction to information. A "**statement of disagreement**" refers to a patient's reasons for disagreeing with a health information custodian who refuses to correct information in the patient's record.
9. Patients have the **right to appeal** a custodian's decision to the Supreme Court.
10. The IPC may **review** any decision, act, or failure to act by a custodian who has been asked to give access to or correct a record by the person who is the subject of the record.

11 Privacy Breach

Introduction

A privacy breach is an unauthorized use, disclosure, alteration, destruction, disposal, loss, or theft of personal health information. A patient who thinks a custodian has collected, used, or shared his or her personal health information not in compliance with HIA can ask the Information and Privacy Commissioner (IPC) for a review.

This chapter includes the following **key concepts**:

1. What is a privacy breach
2. Custodian roles and responsibilities to prevent privacy breaches
3. Custodian roles and responsibilities to respond to privacy breaches
4. Privacy breach review by the IPC

What Is a Privacy Breach?

Personal health information is important. We need to respect patients' right to privacy and take every reasonable step to protect their personal health information.

There are three main causes of privacy breaches:

- Human error, such as the inappropriate disposal of records, emails sent to the wrong person, or loss of physical files or hardware (e.g., USB storage drives).
- Theft by employees or strangers. Thieves usually take computer devices such as laptops or hard drives, but paper files also may be stolen.
- Unauthorized access or disclosure. Examples include failure to control access, malicious or intentional access, accidental loss of information, and carelessness, such as talking about patients in public.

Custodians have roles and responsibilities under the HIA to implement processes and procedures that provide effective prevention and response to a privacy breach. This may include disciplinary measures for custodians and agents who are not following procedures.

(See Health Information Regulations s.13–14.)

If you think a privacy breach may be occurring, or know that one has occurred, you must stop it if possible. Then report it to your supervisor, designated contact person, and custodian.

The custodian is responsible for notifying the patient.

Privacy Breach Prevention

Safeguards

The HIA requires custodians to implement and maintain safeguards to protect the confidentiality of personal health information and the privacy of patients. Safeguards can be grouped into three categories:

- **Administrative safeguards** include written policies and procedures, oaths of confidentiality, privacy awareness training programs, codes of conduct, and access request forms.
- **Technical safeguards** include computer systems and controls such as complex password requirements, audit logs, backup, and role-based access permissions.
- **Physical safeguards** provide security in locations where personal health information is kept. They include locked cabinets, key controls, motion detectors and other intrusion alarm systems, fire suppression equipment, secure shredding procedures, and controlled access to fax machines.

The following administrative, technical, and physical safeguards are required under section 85 of the HIA:

- measures to protect personal health information through an assessment of re-identification risk and the application of de-identification procedures as required
- measures to protect network infrastructure from interruption and unauthorized access and use
- the use of authentication and encryption to protect personal health information stored electronically
- measures to prevent and respond to problems involving hardware and software that might threaten the security, confidentiality, or integrity of personal health information
- measures to protect hardware and software from unauthorized access and use

- measures to protect personal health information stored and transported on removable media
- a requirement that personal health information be maintained in a designated area subject to appropriate security safeguards
- a requirement that access to personal health information be monitored on an ongoing basis for the purpose of ensuring that only authorized access is occurring
- procedures that provide for the recording, reporting, and investigation of security and privacy breaches
- procedures that provide for effective prevention of, response to and remediation of security and privacy breaches

(See *Health Information Regulations s.13(1)(a)-(j).*)

- procedures to recognize privacy or security breaches, contain and mitigate them, notify the individual(s) affected, the Information and Privacy Commissioner and other parties as necessary, and review and respond to breaches

(See *HIA s. 87, Duty to give notice; Health Information Regulations s.14-15.*)



(See [Chapter 2, Custodians and Agents.](#))

Train and monitor all agents to make sure they follow the standards, policies, and procedures that the custodian has established to comply with the HIA. For example, an agent using their privileged access to view their own record or a family member's record is not ethical or professional behavior. Custodians and agents must follow the same processes as other NWT residents in how they request and gain access to their own medical records. You have the right to obtain your information, but you must follow the rules. Having good policies that are implemented and used consistently is the best way to prevent a privacy breach.

Privacy Awareness Overview training prepares everyone in a health care organization to identify a potential or actual privacy breach and protect patients' personal health information. The custodian is responsible for training agents.

Initiate a review of current practices and compliance with the HIA. Review safeguards at least annually to ensure the security of health information. Identify any gaps and prepare an implementation plan that supports compliance with the HIA.

Notify all employees about the changes as part of your implementation plan. Promote organization monitoring so that employees follow practices and policies consistently.

Privacy Impact Assessment

The HIA requires public custodians to prepare a privacy impact assessment (PIA) whenever a new or updated information system or communication technology is considered for the collection, use, or disclosure of personal health information. The PIA is a written document that must be submitted to the IPC.

(See *HIA s.89(2), Privacy impact assessment required; s.89(3), Privacy impact assessment to IPC.*)



(See *Privacy Risk Toolkit, available from DHSS website*

[health-privacy-protecting-your-health-information.](#))

The IPC may provide comments on the PIA to the custodian who submitted the PIA.

(See *HIA s.175, Privacy impact assessments.*)

Privacy Breach Response

An effective privacy breach management program will promote an organized and timely response to a privacy breach incident. Implementing a privacy breach management program will help you:

- Meet your obligations as a custodian.
- Support your agents.
- Maintain the confidentiality of your patients' personal health information.
- Ensure compliance with HIA.

Telling a patient about a privacy breach is difficult. But just as you would want your bank to let you know that your credit card information may have been stolen, the patient will want to know that her or his information was compromised. Most of the time, patients appreciate the notice.

(See HIA s. 87, Duty to give notice; HIA s.134–140, Reviews Relating to Collection, Use and Disclosure of Personal Health Information.)

Some incidents should be reported to IPC and law enforcement officials.

(See Health Information Regulations s.15.)

If a privacy breach occurs, custodians and agents must avoid the following common errors:

- The first error is to ignore the breach. People may be nervous about reporting. They may not want to deal with any paperwork that can be involved. However, all privacy breaches should be reported. Once you have identified a privacy breach, make sure it does not spread any further. Next, notify your supervisor or the designated contact person. You might be required to fill out a Privacy Breach Incident Report.
- The second most common error is not notifying the individual affected by the breach. If people do not know about an incident involving their information, they cannot take steps to protect themselves. The consequences of a breach can become much worse if it is not managed quickly.

- The third error is failure to communicate. Make sure that your staff are aware of the incident and know how to answer questions from patients and the public. The media spokesperson, designated contact person, and custodian must be available to give accurate information about the breach to staff and the public.

Disciplinary actions are frequently applied by the custodian and may include training, warning, and sometimes dismissal. Custodians and agents can also face sanctions from their professional colleges. Corporations that commit offences under the HIA can be charged up to \$500,000. Individuals can be charged up to \$50,000.

Recognize

Recognize a suspected privacy breach and inform your supervisor, the designated contact person, and the custodian. Take immediate common-sense steps to limit the breach:

- Stop the unauthorized access.
- Recover or secure the records and shut down the system that was breached.
- Cancel user accounts, passwords, permissions, keys, etc. to control the security of the information.

Investigate

The designated contact person, with the assistance of the custodian, should:

- Investigate the cause of the privacy breach.
- Initiate the Privacy Breach Report.
- Evaluate the risks associated with the breach, including the risk of harm to the patient (e.g., identity theft) or systemic failure of computer or information systems.

The custodian should review the Privacy Breach Report and authorize immediate steps to mitigate the risks associated with the breach. This could include corrective measures or ad hoc procedure changes until new practices and procedures are developed.

Report

Consider notification to:

- affected individuals, including patients, health service providers, and custodians, as required by HIA, ATIPP, PIPEDA, and contractual obligations
- law enforcement if the breach involves theft or criminal activity
- insurers
- professional or other regulatory bodies
- credit card companies and/or credit reporting agencies
- IPC
- GNWT Risk Management Office
- GNWT Office of the Chief Information Officer
- DHSS

Notify and report the breach as authorized by the custodian to the patient, the IPC, and others. See the *Health Information Regulations* for the latest IPC notification requirements. Reporting a breach to the IPC allows the IPC to support the custodian and designated contact person in responding to the breach.

(See HIA s.87, Duty to give notice; Health Information Regulations s.15.)

Review and implement a communications plan.

- Create and distribute internal and external communication messages.
- Review and update communication messages during the investigation, during notification, and after the breach.

Correct and Mitigate

After taking immediate actions to limit the breach, initiate longer term actions to correct or stop the breach from continuing to occur.

Analyze the risks associated with the breach, including the risk of harm to affected individuals. Have the custodian, management, and risk managers review the Privacy Breach Report and make recommendations for improvement.

Review and update policies and procedures to reduce the risk of future privacy breaches.

Carry out an audit at the end of the breach review process to ensure that the response plan has been fully implemented.



(See the DHSS website [health-privacy-protecting-your-health-information](https://www.health-privacy-protecting-your-health-information.ca) for additional information about privacy breach reporting requirements.)

Example

A health clinic disclosed a patient's health information when medical records were faxed to the patient's employer instead of his new health care provider. The clinic assistant responsible for the disclosure received a written disciplinary warning. Both the clinic assistant and the custodian apologized to the patient.

The custodian reviewed the office's policies and procedures. The custodian implemented additional safeguards to make sure personal health information was sent to and received by the right person or organization.

Privacy Breach Complaints and Review Process

Review Requested by a Patient

A patient who thinks a custodian has collected, used, or disclosed his or her personal health information in contravention of the HIA may ask the IPC for a review. The IPC is independent from government and has the power to review a possible privacy breach by a custodian.

The IPC **must** give a copy of the request to the custodian concerned. The IPC **may** give a copy of the request to any other person or organization that may be affected by the request. The IPC may sever information in a request before giving it to a person or organization to review.

(See HIA s.134, Request for review: collection, use, and disclosure.)

The IPC may, without conducting a full review, refuse a patient's request for any the following reasons:

- It is frivolous or made in bad faith.
- It is trivial.
- The patient is taking unnecessary advantage of the right to a review.
- It concerns a matter that has already been dealt with under the HIA or the ATIPP.

(See HIA s.135, Review by IPC.)

After a patient requests a review for a privacy breach, the IPC may, without conducting a full review, assist the patient and the health information custodian to resolve the matter. A formal or informal **alternative dispute resolution process** may be followed to settle the disagreement. Methods include negotiation, conciliation, mediation, and arbitration. If the matter is resolved, the IPC must make a record of the resolution.

(See HIA s.136, Alternative dispute resolution.)

Privacy Breach Review Initiated by IPC

An IPC who thinks a privacy breach has occurred can begin a review even if the patient did not make a complaint.

Example

The Information and Privacy Commissioner reads an article in the local newspaper. It says files containing personal health information were found at the dump. The IPC thinks many people could be harmed as a result of this privacy breach. She starts an investigation.

The IPC **must** notify the custodian and **may** notify anyone else affected.

The IPC may at any time end a review that he or she initiated. An IPC who stops a review must notify the custodian.

(See HIA s.137, Review initiated by IPC.)

At any time during a review initiated by the IPC, the IPC may use alternative dispute resolution to settle the matter with the custodian. The IPC must make a record of the resolution with the custodian.

(See HIA s.138, Alternative dispute resolution.)

IPC Privacy Breach Report

At the end of the privacy breach review (initiated either by the individual or the IPC), the IPC must prepare a report on any privacy breach review. The IPC may include recommendations, even if she or he decides that no breach occurred. The IPC must include reasons for any recommendations. The report should include results and confirm whether or not the custodian violated the HIA.

(See HIA s.139, IPC report.)

Copies of the IPC report go to the following people:

- the individual (if the review was initiated by him or her)
- the custodian
- the Minister of Health and Social Services
- any person or organization that made representations at the review

(See HIA s.140, Requirement to give copy of report.)



(For more information about the role of IPC in privacy reviews, see [Chapter 9, Information and Privacy Commissioner](#).)

Custodian's Decision on IPC Recommendations

A report by the IPC (*under HIA s.139 or s.146*) may include recommendations for the health information custodian.

Within 30 days after getting the IPC's recommendations, the custodian must tell the following people whether or not she or he accepts these recommendations:

- the IPC
- the person who requested the review
- the Minister of Health and Social Services (HSS)

A custodian who decides not to accept the IPC's recommendations must tell the person who requested the review that he or she has the right to appeal (HIA s.160(1)) the custodian's decision to the NWT Supreme Court.

If the custodian does not respond within 30 days, everyone must assume the custodian does not accept the recommendations. The IPC can share the custodian's response with anyone involved in the review. A custodian who accepts any IPC recommendation must follow it within 45 days of responding.

(See HIA s.156, Custodian's decision: IPC recommendations; s.157, Notice of decision; s.158, Requirement to comply with decision.)

Appeal to Supreme Court

Patients have the **right to appeal** a custodian's decision to the Supreme Court.

A patient who requested any type of review can appeal to the Supreme Court any decision the custodian makes in response to the IPC's recommendations. An appeal to the Supreme Court must be made within 30 days after the patient receives the custodian's response to the IPC's decision. If the custodian does not respond to the IPC's recommendations, the patient has 90 days to appeal to the Supreme Court.

(See HIA s.160, Appeal by individual of decision by custodian.)

The IPC's recommendations cannot be appealed. If the patient believes the IPC based her recommendations on an incorrect assumption made upon review of the evidence gathered, then the patient can appeal that assumption of finding of the IPC's to the Supreme Court. Appeal to the Supreme Court must be made within 30 days of getting the IPC's report.

(See HIA s.159, Appeal by individual of IPC finding: collection, use and disclosure.)

If the IPC (instead of a patient) started a review of a custodian's activities and the custodian decides not to accept any or all of the IPC's recommendations, the IPC may appeal to the Supreme Court. The appeal must be filed within 30 days after the IPC gets the custodian's decision. If the custodian does not respond to the IPC's recommendations, the IPC has 90 days to appeal to the Supreme Court.

The IPC is not a party in a Supreme Court appeal case unless the IPC started the review.

(See HIA s.161, Appeal by IPC of decision by custodian.)

On an appeal, the Supreme Court shall make its own determination of the matter. The Supreme Court can examine any record held by the custodian. No one can withhold evidence. The Supreme Court can share information with law enforcement if it thinks a crime has been committed.

(See HIA s.165, Disclosure of information relating to offence.)

The Supreme Court can make any order and set any conditions it considers appropriate. An order of the Supreme Court is final and cannot be further appealed apart from a review of court process during the appeal. A person or organization shall comply with an order within the time set in the order, or if no time is set, within 45 days after the order is issued.

(See HIA s.167, Order of Supreme Court.)

Resources

These resources are available from DHSS website [health-privacy-protecting-your-health-information](#).

Health Information Regulations - privacy breach reporting requirements.

Privacy Risk Toolkit

Roles and Responsibilities of Designated Contact Persons – Video

What to Do in Case of a Privacy Breach – Video

Selected references and resources that were used in the development of Chapter 11, Privacy Breach

Canada. Office of the Privacy Commissioner of Canada.

- [Privacy Breach Checklist](#)
- [Privacy Toolkit. A Guide for Businesses and Organizations Canada's Personal Information Protection and Electronic Documents Act](#)

Canada. Office of the Privacy Commissioner of Canada and Offices of the Information and Privacy Commissioners of Alberta and British Columbia. (April 2012).

- [Getting Accountability Right with a Privacy Management Program](#)
- [Securing Personal Information: A Self-Assessment Tool for Organizations Authors](#)

Chapter 11. Privacy Breach – Test Your Knowledge

The following quiz applies many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 179](#).

1. Privacy breaches include which of the following?
 - a. unauthorized collection
 - b. unauthorized use
 - c. unauthorized sharing of personal health information
 - d. loss of personal health information
 - e. any of the above
2. Which of the following are examples of a privacy breach?
 - a. agent discloses the health care number of a patient to the patient's school without the express consent of the patient
 - b. looking up your friend's birthdate on the EMPI
 - c. patient's referral letter is faxed to a store instead of his family physician's office
 - d. a paper with patient information is put in the garbage instead of secure shredding
 - e. nurse faxes a patient's referral to the allergy specialist
 - f. billing clerk accesses a patient's medical record to confirm the treatments billed were the ones provided
3. What are custodians' roles when preventing or responding to a privacy breach?
 - a. Custodians are responsible for notifying a patient whose personal health information has been breached.
 - b. Custodians do not need to gather evidence when a privacy breach occurs.
 - c. Custodians should develop and implement procedures that effectively prevent and manage privacy breaches.
 - d. Custodians must consider appropriate discipline in the event of a privacy breach.
 - e. All of the above.
4. A person can contact the IPC and request a review of a potential breach.
 - a. true
 - b. false

Chapter 11. Privacy Breach – Summary of Key Concepts

1. A **privacy breach** is the unauthorized collection, use, or disclosure of personal health information, or the loss, theft, or destruction of personal health information.
2. There are **three main causes of privacy breaches**: human error, theft by employees or strangers, and unauthorized access or disclosure.
3. If you learn of a privacy breach, stop it if possible. **Report** the incident to your supervisor or designated contact person and custodian. The custodian is responsible for notifying the patient.
4. Privacy breaches can be prevented by the use of administrative, technical, and physical **safeguards**.
5. Safeguards must be implemented to prevent a privacy breach. **Safeguards** must be reviewed as needed and at least annually.
6. The HIA requires a public custodian to prepare a **Privacy Impact Assessment (PIA)** whenever a new or updated information system or communication technology is considered for the collection, use, or disclosure of personal health information. This PIA must be submitted to the IPC.
7. Privacy Awareness Overview **training** prepares everyone in a health care organization to identify a potential or actual privacy breach and protect patients' personal health information.
8. A patient who thinks a privacy breach has occurred involving her or his personal health information, can ask the **IPC to review** the situation.

12 Offences and Limitation of Liability

Introduction

The *Health Information Act* (HIA) was enacted to protect personal health information. There are strong enforcement measures in place to ensure the HIA is followed. The HIA specifies penalties for various offences.

This chapter includes the following **key concepts**:

1. Offence and penalties
2. Limitation of liability

Offence and Penalties

Offences

No person shall knowingly collect, use, or disclose personal health information in contravention of the HIA or the regulations.

No one must interfere with or mislead the IPC, custodians, or Supreme Court.

No one must fail to follow a requirement set by the IPC, custodian, or Supreme Court.

No one must alter, falsify, conceal, or destroy a record intentionally to avoid an access or correction request or to avoid sharing the information.

No one must pretend to be someone else to access or change someone's information.

No one can use a person's health information to market a service, solicit money, or any other commercial purpose unless that person has given her or his express consent.

No person shall knowingly contravene or fail to comply with the HIA or the regulations.

(See HIA s.185, Prohibition: collection, use and disclosure; s.186, Prohibition: obstruction; s.187, Prohibition: alteration, falsification, concealment or destruction; s.188, Prohibition: false representation; s.189, Prohibition: commercial purpose; s.190 General prohibition.)

Penalties

Corporations that commit offences under the HIA can be penalized up to \$500,000. Individuals can be penalized up to \$50,000. These fines are higher than those charged under the ATIPP. They are consistent with other health privacy legislation.

If a corporation commits an offence, any officer, director, agent, or employee of the corporation who was involved in committing the offence can be charged and convicted.

A charge can be laid within 3 years of the offence.

(See HIA s.192, Offence and punishment; s.193, Officers of corporation; s.194, Limitation period.)

Limitation of Liability

"Acting in good faith" means behaving honestly and doing what you believe is in the best interest of others. Taking action that you believe follows the Act is an example of acting in good faith.

"Liability" means the legal responsibility for something. The Government of the Northwest Territories and its officers and employees are immune from liability if they act in good faith. Custodians and their agents are not legally responsible for sharing or not sharing health information under the HIA if they honestly believe that they are acting in good faith.

The following are not liable when they act in good faith:

- Government of the Northwest Territories
- health information custodians
- agents
- Information and Privacy Commissioner (IPC)
- IPC staff
- those giving evidence in accordance with the HIA

No one can be sued for doing something the IPC asked, required, or recommended.

(See HIA s.180, Immunity from liability; s.181, Immunity from liability: IPC; s.182, Immunity from liability: provider of information; s.183, Prohibition against penalizing agent; s.191, Immunity from prosecution.)

Resources

These resources are available from DHSS website [health-privacy-protecting-your-health-information.](#)

Health Information Act

Health Information Regulations

Chapter 12. Offences and Limitation of Liability – Test Your Knowledge

The following quiz applies many of the key concepts in this section. Circle the answer(s) for each question. Then check your answers with the answer key on [page 180](#).

1. Which of the following individuals are immune from liability if they act in good faith?
 - a. Information and Privacy Commissioner
 - b. custodian
 - c. provider of information
 - d. all of the above
2. Interfering or misleading the Information and Privacy Commissioner, custodians, or Supreme Court is an offence under the Act.
 - a. true
 - b. false

Chapter 12. Offences and Limitation of Liability – Summary of Key Concepts

1. The custodians, agents, IPC and providers of information have **immunity from liability** as long as their actions were taken or not taken in good faith.
2. The Act serious **penalties** for offences related to the collection, use, and disclosure of information; interfering or giving misleading information; and destroying or falsifying a record.
3. **Corporations** that commit offences under the HIA can be fined up to \$500,000.
4. **Individuals** can be fined up to \$50,000.

Resources

Introduction – Resources

Orientation Checklist for Employees

You may use the *Health Information Act Guide* as part of your orientation program. Use the sample form on the next page to identify the sections of the guide that new employees should read. You can ask employees to read all or only certain sections of the guide.

Instruct employees to:

- Read the selected sections of the *Health Information Act Guide*.
- Initial the sections they have completed.
- Sign the checklist.
- Return it to their supervisor.

How to Read an Act

Use this quick-tip guide to learn how to find information in the *Health Information Act* and properly reference sections of the Act.

Orientation Checklist for Employees

- ☐ Reviewed relevant parts of the *Health Information Act Guide* (supervisor to indicate required parts):
 - ☐ Introduction to the *Health Information Act Guide*
 - ☐ Scope of the Act
 - ☐ Custodians and Agents
 - ☐ Consent
 - ☐ Collection
 - ☐ Use
 - ☐ Disclosure
 - ☐ Disclosure for Research and Research Ethics Committee
 - ☐ Information Managers and Information Management Agreements
 - ☐ Information and Privacy Commissioner
 - ☐ Access and Correction of Personal Health Information
 - ☐ Privacy Breach
 - ☐ Offences and Limitation of Liability
 - ☐ Resources
 - ☐ Answer Keys to Test Your Knowledge
 - ☐ Links to the Act
 - ☐ Index
- ☐ Completed Test Your Knowledge and compared it to the Answer key
- ☐ Reviewed Summary of the Key Concepts

Employee signature

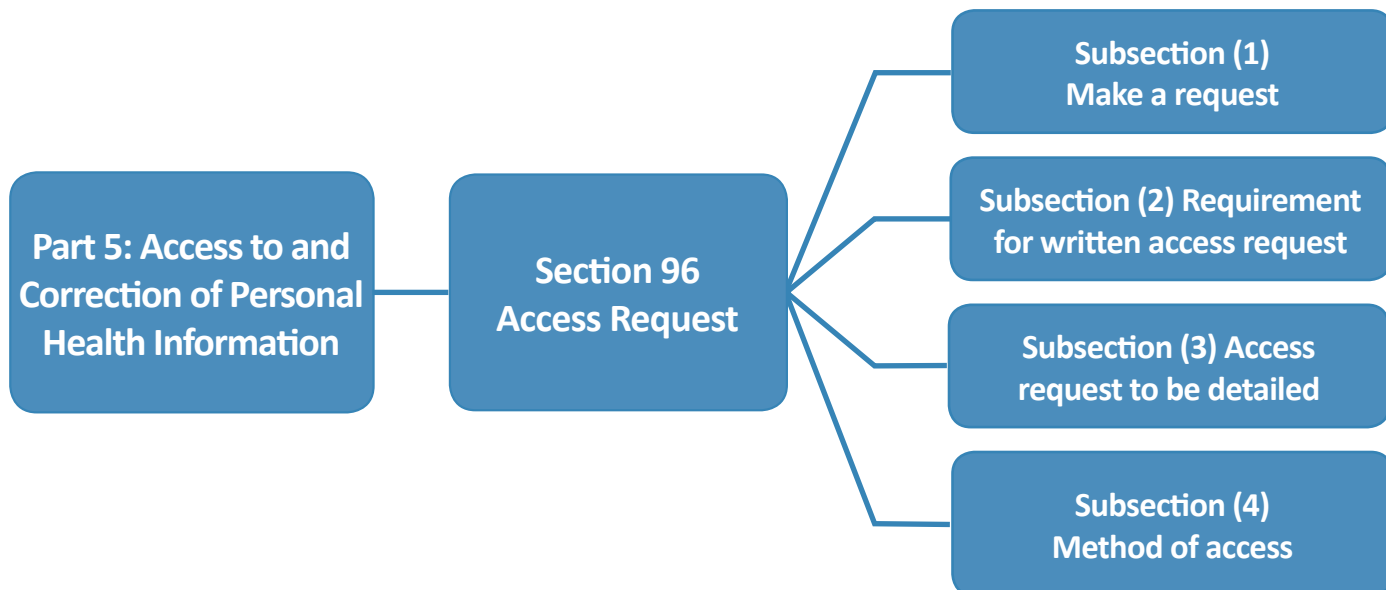
Date

Supervisor signature

Date

[Copy and save to Human Resources file]

How to Read an Act



Laws, also called **Acts and Regulations**, are highly structured documents. Once you understand that structure, it becomes much easier to find your way around and between them.

The **title page** and **table of contents** help you find the information you are looking for.

The main body, or text of the law, is divided into a number of different parts. Those parts are then broken down by section and subsection.

Next, after the section there may be a **subsection**, then a **paragraph** and under that, a **sub-paragraph**.

For most legislation, including Acts, a large portion of information will be under “**section**”, and it is usually cited as ‘s’ for a section, and ‘ss’ for subsections.

In addition, there may be Schedule at the end of the main body. Schedules often contain details like tables or lists of items or amendments, and might also contain headings. Schedule numbering varies so you may see Schedule 1, Schedule A and even First Schedule.

The most important point to remember is that when you read the Table of Contents, the numbers following the topic refer to the section numbers in the Act, not the page number.

For example: the reference in the Act on “requirement for written access request” is:

HIA Part 5 s.96(2) or HIA s.96(2). This is spoken as, “HIA, section 96, subsection 2” or “section 96, sub 2”.

Chapter 1. Scope of the Act – Resources

Does the HIA Apply? – Infographic

Use the infographic to help you to determine whether the *Health Information Act* applies to a particular patient and situation.

Does the HIA Apply? – Infographic

Does the *Health Information Act* (HIA) Apply?

1. Is there personally identifying health information?

See HIA s.1(1),
personal health information (a–i).

Personally identifying health information

- Person's name and contact information
- Personal health number or other identifying health number or symbol assigned to a person receiving health services or information
- Information used to determine whether a person is eligible for a health service or benefit or to register a person for a health service or benefit
- Prescription information
- Information used to determine if a person qualifies for Extended Health Benefits (EHB) or an escort during medical travel
- Information about payment for a person's health service
- Information about donation of a person's body part or substance
- Information about a health service provided to a person

2. Is there a custodian?

See HIA s.1(1),
health information custodian
and public custodian.

Custodians named in the HIA

- Department of Health and Social Services (DHSS)
- Private physicians
- Health and Social Service Authorities (HSSAs)
- Private pharmacists

3. Is there a health service?

See HIA s. 1(1),
health service (a)(i–iv).

Health services

Any observation, examination, assessment, or procedure for the following purposes:

- Protection, promotion, or maintenance of health
- Diagnosis
- Testing or examination of a body part or substance, e.g., laboratory test or x-ray
- Treatment or rehabilitation
- Prevention of conditions adverse to health
- Care for people who are ill, injured, disabled, or dying
- Ambulance service
- Organ and tissue donation and transplant
- Mental health services
- Addiction services, e.g., treatment, counselling, and detoxification

**The *Health Information Act* applies
if the answer to all three questions is “Yes.”**

Chapter 2. Custodians and Agents – Resources

Custodian Responsibility Checklist

Custodians under the Act must ensure their agents follow the standards, policies, and procedures outlined in the HIA. Use this quick-tip guide to learn how to assess your current practices and identify areas in which they could be improved.

Sample Oath of Confidentiality

An Oath of Confidentiality for agents and custodians could be based on this template. Custodians may modify and develop your own document. This sample form includes a statement that the person will respect privacy, has received training and can ask questions his or her supervisor.

Custodian Responsibility Checklist

Now that you've read Chapter 2, and you know your responsibilities as a custodian, the next step is to develop your own checklist. This quick-tip guide may assist you to assess your current practices and identify areas in which they could be improved. The list is organized into four areas, as introduced in Chapter 2:

1. Policies, Standards, and Procedures

- ☐ Share the custodian's policies and procedures with the DHSS if requested.
- ☐ Keep records to document that policies and procedures are being followed.
- ☐ Review and update policies and procedures regularly, at least annually.
- ☐ Instruct and ensure agents follow the standards, policies, and procedures set by the custodian.
- ☐ Instruct and ensure agents follow the HIA.
- ☐ Explain to agents that they are authorized by you, a custodian, to do work that involves collecting, using, and sharing patients' personal health information. Agents must follow the rules and always respect patients' privacy.
- ☐ Instruct and ensure agents that they must not collect, use, disclose, manage, retain, or destroy personal health information unless they are allowed to under the HIA and by you, a custodian.

2. Safeguards

- ☐ Document current practices and compliance with the HIA.
- ☐ Identify any gaps and prepare an implementation plan.
- ☐ Conduct an annual review of compliance and effectiveness of safeguard measures in place.
- ☐ Develop and implement procedures to prevent and respond to privacy and security breaches.
- ☐ Implement controls to protect personal health information against unauthorized access, use, disclosure, or alteration. Assess re-identification risk and apply de-identification procedures or techniques, as applicable, to transform personal health information into non-identifying health information in accordance with section 36 of the Act.
- ☐ Protect network infrastructure, including physical and wireless networks, from interruption and unauthorized access and use.
- ☐ Protect personal health information stored electronically, including through the use of authentication and encryption.
- ☐ Prevent and respond to problems involving hardware and software, including power failure, that threaten the security, privacy, or integrity of health information or that might result in the loss of health information.
- ☐ Protect hardware and software from unauthorized access and use.
- ☐ Protect personal health information stored and transported on removable media, such as:
 - ☐ secure storage of the media device when not in use
 - ☐ deletion of the information when the media device is no longer in use
 - ☐ use of authentication and encryption

- ☐ Maintain personal health information in a designated area subject to appropriate security safeguards, including safeguards to ensure that only authorized persons have access to those areas.
- ☐ Monitor access to personal health information on an ongoing basis for the purpose of ensuring that only authorized access is occurring.

3. Additional Requirements

- ☐ Ensure access to records with the use of organized records management systems.
- ☐ Conduct a Privacy Impact Assessment (PIA) whenever a new or updated information system or communication technology is considered for the collection, use, or disclosure of personal health information. Public custodians must submit the PIA to the Information and Privacy Commissioner.
- ☐ Provide notices to patients on how their information may be used or shared; provide notices:
 - ☐ Upon registration and prior to collecting patient's personal health information
 - ☐ In reception areas or other areas where patients are likely to see the notice.
 - ☐ In more than one format which may include:
 - written (posters, forms, brochures)
 - verbal
 - multi-media (audio and visual)
- ☐ Develop and maintain procedures for tracking and responding to access requests.
- ☐ Post instructions on how to contact the designated contact person for information, questions, or concerns.

4. Training

Custodians should train and monitor all agents to make sure they follow HIA standards, policies, and procedures in place to support compliance with the HIA. To do this, you as custodian can provide:

- ☐ on-the-job orientation
- ☐ privacy awareness overview training
- ☐ access to policies and procedures
- ☐ mentor, supervise, and monitor employees' work to make sure they follow the standards, policies, procedures, and safeguards developed to comply with the HIA.
- ☐ compliance reviews
- ☐ training records and acknowledgement that training has been delivered, received, and key concepts are understood / demonstrated on the job

5. Designated Contact Person

You, as a custodian must name at least one agent as the designated contact person. The contact person is someone in the organization, clinic, or health centre who understands the HIA and its regulations. This person must be familiar with your- custodian's privacy policies and procedures.

☐ Our designated contact person is: _____

The contact person has the following responsibilities:

- ☐ Promote staff compliance with the HIA.
- ☐ Respond to questions and complaints from the public about the collection of information, and information practices.
- ☐ Process and respond to access and correction requests.
- ☐ Receive complaints about non-compliance with the HIA.
- ☐ Act for the custodian in dealings with third parties and the Information and Privacy Commissioner.
- ☐ Investigate, mitigate, and remediate privacy breaches.

As you develop your checklist, you may include additional information at the bottom for e.g.:

Comments / Recommendations: _____

Checklist completed by: _____

Date: _____

Next Review: _____

Reviewed by Custodian: _____

Date: _____

Sample Oath of Confidentiality

An Oath of Confidentiality for agents and custodians could be based on this template. It is for you to modify and develop your own document. This sample form includes a statement that the person who signs the oath has received training and can ask questions his or her supervisor.

1. I, _____ agree that I will faithfully discharge my duties as an employee / volunteer / contracted service provider for the custodian, and will observe and comply with all policies and procedures of the custodian with respect to privacy, confidentiality, and security of health information.
2. I have received and read the custodian's specific Information Handling and Security practices which includes:
 - a. Information Handling and Security procedures
 - b. Laptop Security
 - c. Wireless Networking / Remote Access policies
3. Unless legally authorized to do so, I will not use or disclose health information that comes to my knowledge or possession by reason of my affiliation with the custodian, including after I cease to be employed by the custodian.
4. I understand that a breach of this agreement may be just cause for termination of my employment or affiliation with the custodian.
5. I am aware that the custodian has policies and procedures regarding the privacy, confidentiality, and security of health information and it is my responsibility to be familiar with the requirements outlined in these policies and procedures.
6. My use of the custodian's electronic medical record, central patient index, and other electronic applications may be monitored to ensure appropriate confidentiality, and security. Specifically, audit and access logs will be checked by the system administrator if a breach of security or privacy is suspected. The custodian will work with the vendor to automatically generate audit logs that identify use of the system outside of office hours, same last name (of user and patient record look-up), and similar monitoring criteria.
7. I understand that I can refer to the custodian or the designated contact person for the details of these policies and any other information required for me to understand my obligations.

Signature

Printed Name

Date

Chapter 3. Consent – Resources

Notice of Collection of Personal Health Information

Sample notices that you can customize and use in your practice.

Notification of Collection of Personal Health Information

The custodian is required to provide notice of the purpose of collection, use, and disclosure of personally identifying health information. The notice must include the legal authority to collect, use, and disclose this information.

Below is a sample notice that you can customize and use in your organization.

There are many ways that you can provide notice to patients – posters in the reception area, examination rooms, closed circuit TV, new patient welcome brochure, discussion with patient.

Collection Notice

When you receive health services of any kind from this clinic, we collect individually identifying health information from you and share this within the clinic and with other health service providers that need the information to provide you with health services.

The individually identifying health information that you provide to us is collected, used and disclosed in accordance with the provisions of the *Health Information Act* (HIA s.15), and is primarily used to provide diagnostic, treatment and care services to you.

The privacy provisions of the legislation require that we protect your health information from unauthorized access, use, disclosure or destruction.

If you have any questions, please contact:

the Clinic Manager, _____ Phone _____

or our designated contact person, _____ Phone _____

Chapter 4. Collection – Resources

Sample Consent to be Photographed/Recorded and Sample Policy/Procedure

Policy: Safeguards when using a recording device

Before a health information custodian collects personal health information using a recording device, camera or other device that records information in a manner that may not be obvious to the individual from whom information is to be collected, the custodian shall inform that individual that the device will be used.

To ensure that the patient understands that they are being recording, getting a signature from the patient confirming they have been informed is a good practice.

The custodian will ensure that there are good safeguards in place to protect the privacy, confidentiality, and security of the personal health information collected using a recording device. This includes using only authorized custodian-owned and managed recording equipment. Only specially designated recording devices will be used; personal recording devices of patients or employees (personal cell phones, recorders, etc.) will not be used for this purpose.

The images are encrypted and saved to the custodian's computer network servers. The camera is restricted to office use and is locked in an office. When not in use, the memory card is stored in a separate location. All of the existing digital pictures will be transferred to the specific chart at that time or if this is not possible, cross-reference will be recorded in the patient record to ensure a complete patient record.

Sample Consent to be Photographed/Recorded

Custodian: _____
(name)

Consent to be Photographed / Video Recording / Audio Recording

I, _____, give my consent for the taking of
☐ Photographs (still images) ☐ Video Recording ☐ Audio Recording

by _____. I understand that these recordings will be used by
(name of photographer or name of custodian)

Counsellor, _____ and _____
(custodian)

to assist in the care, treatment or diagnosis of my condition, and that no information which might reveal my personal identity shall be revealed to anyone other than those who are directly responsible or involved with my care.

I also understand that these recordings will not be reprinted, published or otherwise reproduced in any scientific or academic journal or book or any other publication, or other means of reproduction, without my further written authorization. This includes transmission by any electronic means to any permission except a person who is directly involved with my care.

(Patient's name)	(Guardian's Name)
(Patient's signature)	(Guardian's Signature)
Date	Date
Date of recording(s):	
Patient's full name(s):	
Date of birth:	
NWT Healthcare Plan Number:	
Patient Record Number:	

Acknowledgement: Rozovksy, Lorne E. *Canadian Healthcare Forms and Policies*. Lexis Nexis 2007.

Chapter 5. Use – Resources

Use of Personal Health Information at-a-Glance

Use this guide to assist you to respond to frequently asked questions (FAQ) regarding the use of personal health information for authorized (secondary) uses.

Use of Personal Health Information at-a-Glance

Use this guide to assist you to respond to frequently asked questions (FAQ) regarding the use of personal health information for authorized (secondary) uses. For more information, see Chapter 5, Use, in the *Health Information Act Guide*, or the HIA.

Use	Explanation
To provide health services	<p>Personal health information that was originally collected or subsequently used at a later date for the purpose of diagnosis, treatment and care of an individual.</p> <p><i>(See HIA s.35(b), Use by custodian.)</i></p>
To determine or verify eligibility to receive a health service or benefit	<p>To determine or verify eligibility to receive a health program, service or benefit. Personal health information may be used for medical travel, and during the application and eligibility verification process to receive benefits and become part of a health program, such as the Extended Health Benefits program or Non-Insured Health Benefits.</p> <p><i>(See HIA s.35(c), Use by custodian.)</i></p>
For internal management related to health services delivery	<p>For internal management purposes including:</p> <ul style="list-style-type: none"> • planning and resource allocation • policy and procedure development • monitoring, chart auditing, evaluation, and reporting • quality improvement • legal services, error management services and risk management services • training and mentoring <p><i>(See HIA s.35(d) (i-iv; vi-vii), Use by custodian.)</i></p>
For billing	<p>A custodian may use personal health information to submit or process a claim for billing.</p> <p><i>(See HIA s.35(d)(v), Use by custodian.)</i></p>
For an inspection	<p>A custodian may use personal health information to carry out an inspection, investigation or review of a health facility.</p> <p><i>(See HIA s.35(e), Use by custodian.)</i></p>

Use	Explanation
For research	<p>A custodian may use personal health information for research; however the custodian must comply with the research requirements set out in the HIA. Specifically, to carry out research, a custodian must receive approval from the HIA designated research ethics committee (REC), the Aurora College REC, and sign a research agreement. Internal management and health system planning are not research, unless it is personal or academic.</p> <p><i>(See HIA s.35(f), Use by custodian; HIA s.67-83, Collection, use and disclosure of personal health information for research purposes.)</i></p>
To seek patient consent	<p>A custodian may use a patient's name and contact information on file to contact the patient for the purpose of seeking the patient's consent, for example to get their consent to share their information with a researcher.</p> <p><i>(See HIA s.35(g), Use by custodian.)</i></p>
For another specific purpose	<p>A custodian has collected or created personal health information for a specific purpose. A custodian may only use that information for the purpose for which it was collected or created and for all functions necessary to carry out that purpose.</p> <p><i>(See HIA s.35(a), Use by custodian.)</i></p>
To de-identify information and for data matching	<p>A custodian can de-identify personal health information to make it non-identifying.</p> <p>A custodian may match data if they have properly collected the information and use the information for a purpose authorized by the HIA.</p> <p><i>(See HIA s.36(1), Transformation of information; HIA s.36(2), Data matching.)</i></p>
For health system planning and management, public health, and administration and enforcement of the HIA	<p>DHSS and HSSAs can also use personal health information to:</p> <ul style="list-style-type: none"> • develop, manage, and plan health programs and services • plan and allocate resources • evaluate and monitor health services • promote public health and for public health surveillance • administer and enforce the HIA <p><i>(See HIA s.37, Additional uses by public custodian.)</i></p>

Chapter 6. Disclosure – Resources

Disclosure of Personal Health Information at-a-Glance

Use this guide to assist you to respond to frequently asked questions (FAQ) regarding the disclosure of personal health information. For more information, see [Chapter 6, Disclosure](#), in the *Health Information Act Guide*, or the HIA.

Disclosure Decision Tree

Use this illustration to assist you to process common requests for disclosure of personal health information with or without the express consent of the patient. For more information, see [Chapter 6, Disclosure](#), in the *Health Information Act Guide*, or the HIA.

Disclosure of Personal Health Information at-a-Glance

Use this guide to assist you to respond to frequently asked questions (FAQ) regarding the disclosure of personal health information. For more information, see Chapter 6, Disclosure, in the *Health Information Act Guide*, or the HIA.

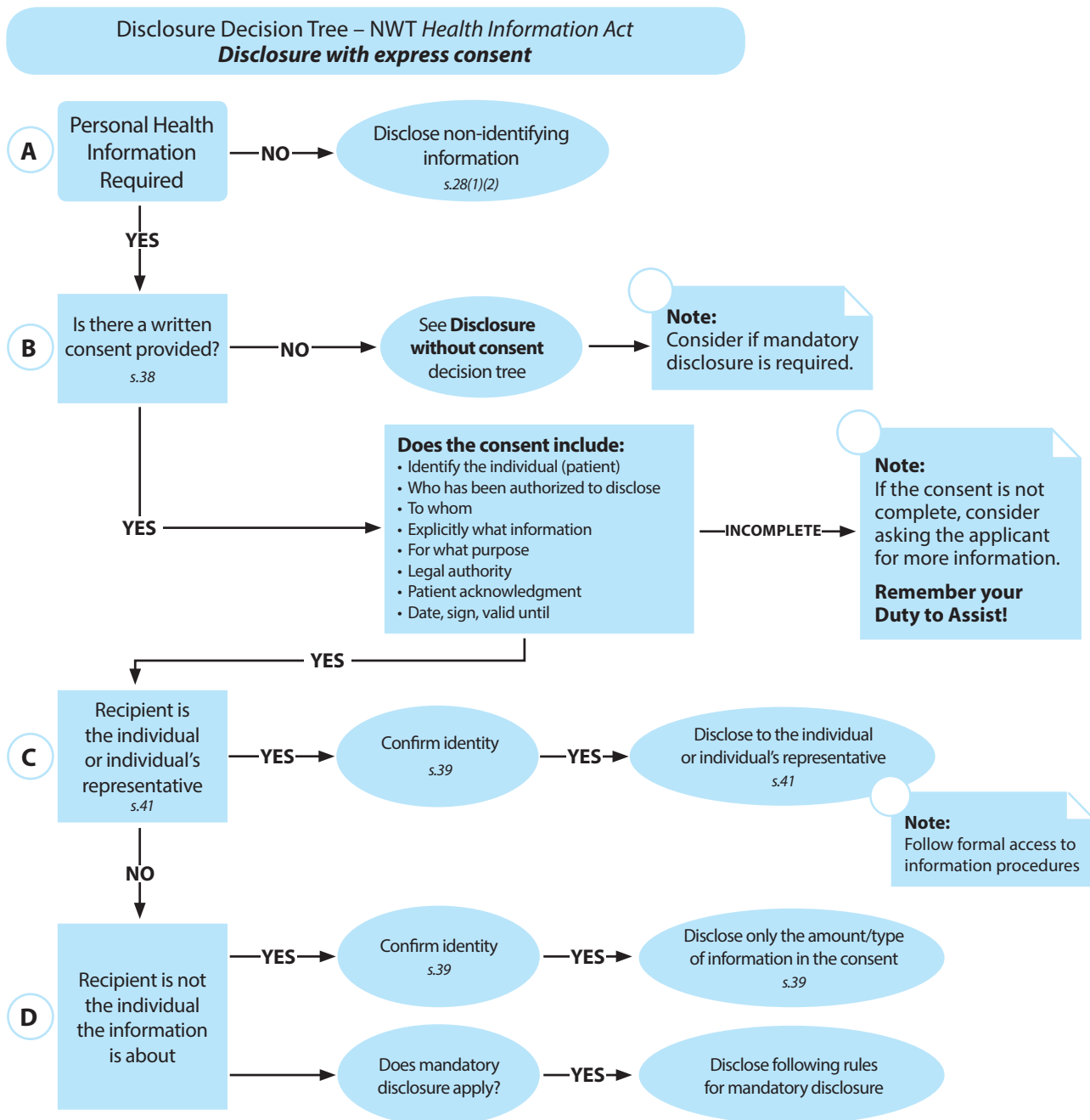
Requestor	Explanation
Any person within the NWT providing care to the patient	<p>Personal health information of an individual may be disclosed to another health service provider for the purposes of treatment and care.</p> <p><i>Discretionary disclosure. (See HIA s.44, Disclosure for health service.)</i></p>
Any person outside the NWT providing care to the patient	<p>Personal health information of an individual may be disclosed to another health service provider for the purposes of treatment and care.</p> <p><i>Discretionary disclosure. HIA s.44(1) is the main provision under which personal health information may be shared with Alberta health service providers when patients travel to Alberta for treatment.</i></p>
Contact purposes	<p>If a custodian cannot get consent from a patient because they are injured or incapacitated, the custodian may disclose some personal health information in order to find a potential substitute decision maker. The disclosure may not be limited to patient's known family.</p> <p><i>Discretionary disclosure. (See HIA s.45, Disclosure for contact purposes.)</i></p>
Relative or person with a close personal relationship to the patient	<p>Custodians can share personal health information in general terms such as location, diagnosis, and/or condition of a patient to the requestor as long as they have verified the person's identity and only if the patient did not give any express instruction to keep it private.</p> <p><i>Discretionary disclosure. (See HIA s.46, Disclosure about patient.)</i></p>
Relative or friend of a deceased patient	<p>Personal health information about a deceased individual may be shared by custodians for reasons such as:</p> <ul style="list-style-type: none"> • identifying the deceased individual, • informing the relative or someone with close personal relationship of the patient's death and/or services provided to them, • enabling a personal representative to settle the patient's estate and • allowing a relative to make health decision about themselves or their child. <p><i>Discretionary disclosure. (See HIA s.47(2), Disclosure about deceased individual.)</i></p>

Requestor	Explanation
<p>Health services delivery:</p> <ul style="list-style-type: none"> • DHSS Billing and health program eligibility • Processing, monitoring or reimbursing claims for payment for health services • Reciprocal billing across jurisdictions 	<p>Custodians can share personal health information about an individual for the purpose of determining eligibility or payment of health services.</p> <p><i>Discretionary disclosure. (See HIA s.48, Disclosure: health services delivery.)</i></p>
<p>Risk to public safety, emergency, or timely investigation</p>	<p>A custodian may share patient health information with a law enforcement agency, including the RCMP, for law enforcement purposes.</p> <p><i>Discretionary disclosure. (See HIA s.57, Disclosure: law enforcement.)</i></p>
<p>Workers' Safety and Compensation Commission</p>	<p>Personal health information can be disclosed to the Workers Compensation Commission, if required. This disclosure occurs if an individual is a worker who receives health care treatment under the <i>Workers' Compensation Act</i>.</p> <p><i>(See WCA s.25, Report by health care provider.)</i></p>
<p>Public health reporting</p>	<p>Custodians have to share patient health information with public health authorities if a law requires this disclosure in order to protect public health.</p> <p><i>Mandatory disclosure. (See HIA s.66, Other public health authority.)</i></p>
<p>Information and Privacy Commissioner</p>	<p>Disclosure must occur if it is necessary for the performance of the IPC's duties.</p> <p><i>Mandatory disclosure. (See HIA s.42, Disclosure to IPC.)</i></p>
<p>Auditor, investigator, quality assurance committee, complaints officer</p>	<p>Disclosure may occur to anyone with legal auditor statutory authority, including the Auditor General of Canada and the NWT Audit Bureau, to a quality assurance committee, to an official inspector or investigator, and to a complaints officer, board of inquiry or other official reviewing a complaint against a health professional.</p> <p><i>Discretionary disclosure. (See HIA s. 49, Disclosure: disciplinary proceedings; s.50, Disclosure: proceedings; s.53, Disclosure: audit, legal services, risk management.)</i></p>

Requestor	Explanation
Legal proceeding	<p>Disclosure of personal health information about an individual may occur without the patient's consent by for the purposes of complying with:</p> <ul style="list-style-type: none"> • subpoena or subpoena <i>duces tecum</i> or • warrant or • order <p>made by a NWT court, person or body having jurisdiction to compel the production of information.</p> <p><i>Discretionary disclosure. (See HIA s.50, Disclosure proceedings.)</i></p>
International Requestor	<p>All disclosure requests received from someone outside of the Northwest Territories should be forwarded to the designated contact person, and reasonable safeguards to be implemented. Need authorization to release information.</p> <p><i>Discretionary disclosure.</i></p>
Member of the Legislative Assembly	<p>Personal health information about an individual disclosed to an MLA by a custodian must have the express consent of individual.</p> <p><i>(See HIA s.20, form of express consent.)</i></p>

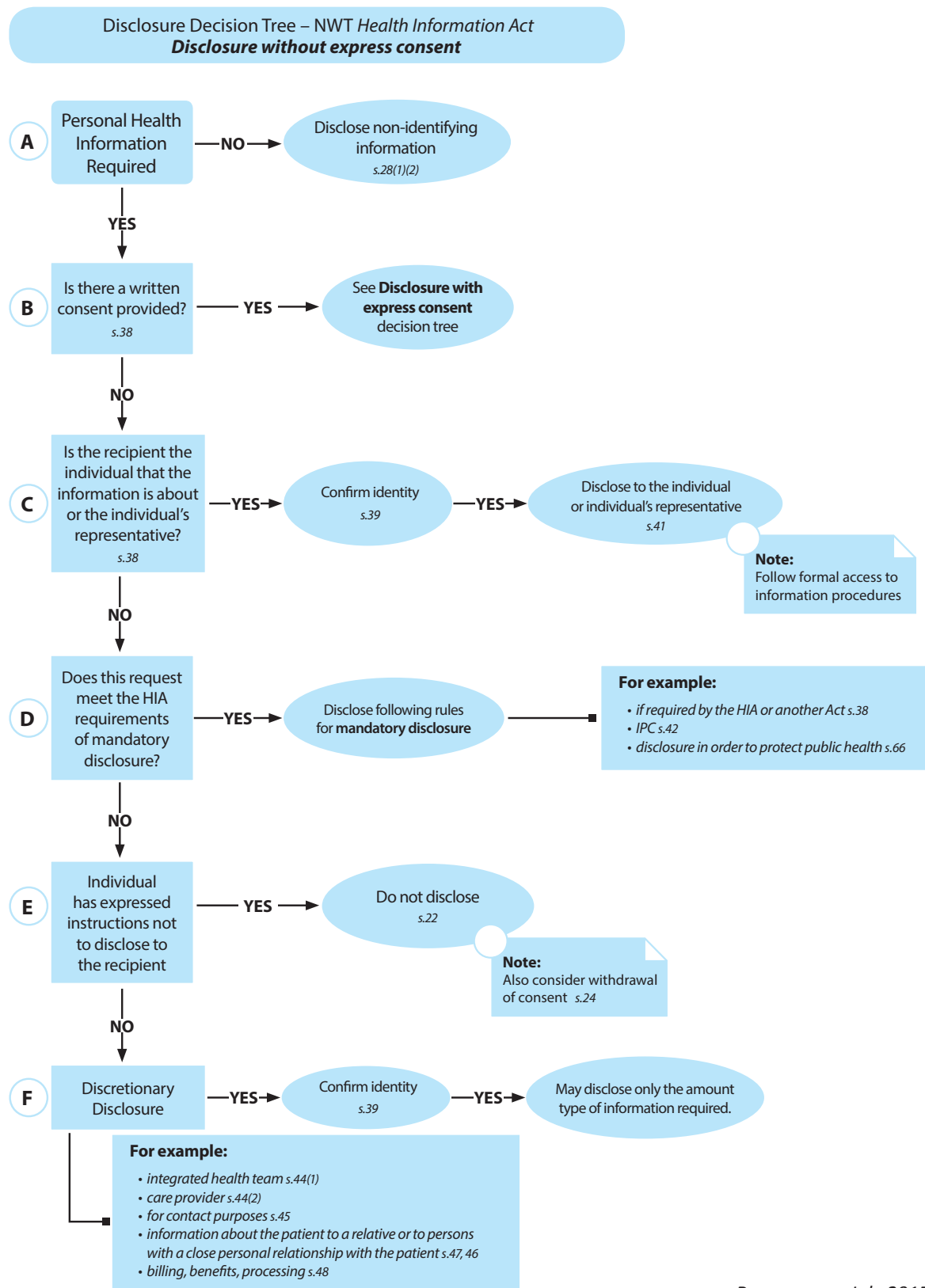
Disclosure Decision Trees – Disclosure with Express Consent

Use this illustration to assist you to process common disclosure of personal health information requests with the express consent of the patient. For more information, see Chapter 6, Disclosure, in the *Health Information Act Guide*, or the HIA.



Disclosure Decision Trees – Disclosure without Express Consent

Use this illustration to assist you to process common disclosure of personal health information requests with the express consent of the patient. For more information, see Chapter 6, *Disclosure*, in the *Health Information Act Guide*, or the HIA.



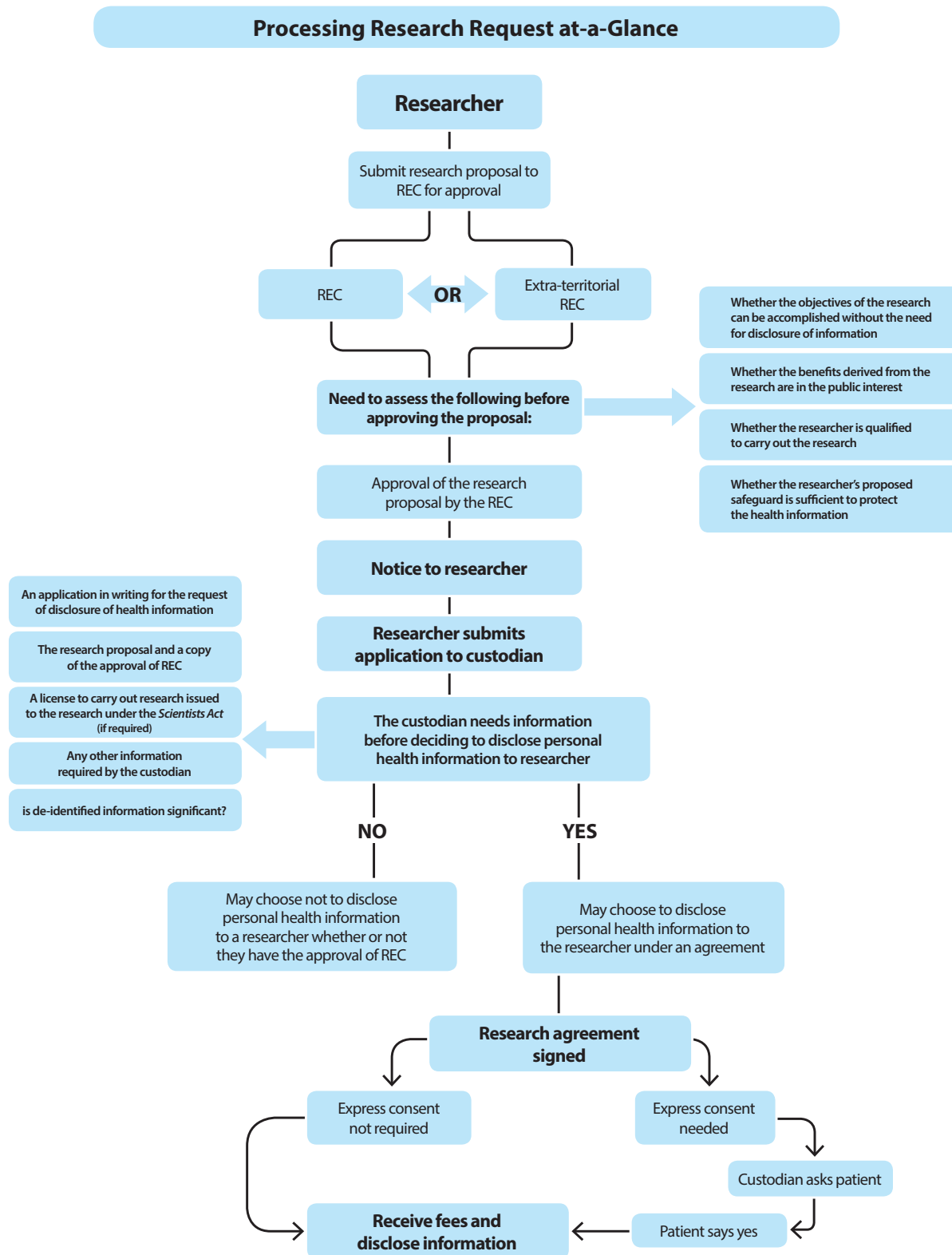
Chapter 7. Disclosure for Research and Research Ethics Committee – Resources

Processing Research Requests at-a-Glance

Use this quick tip guide to assist you process research requests of personal health information. For more information, see [Chapter 7, Disclosure for Research and Research Ethics Committee](#), in the *Health Information Act Guide*, or the HIA s.67-83.

Processing Research Requests at-a-Glance

Use this quick tip guide to assist you process research requests of personal health information. For more information, see [Chapter 7, Disclosure for Research and Research Ethics Committee](#), in the *Health Information Act Guide*, or the HIA s.67-83.



Chapter 8. Information Managers and Information Management Agreements – Resources

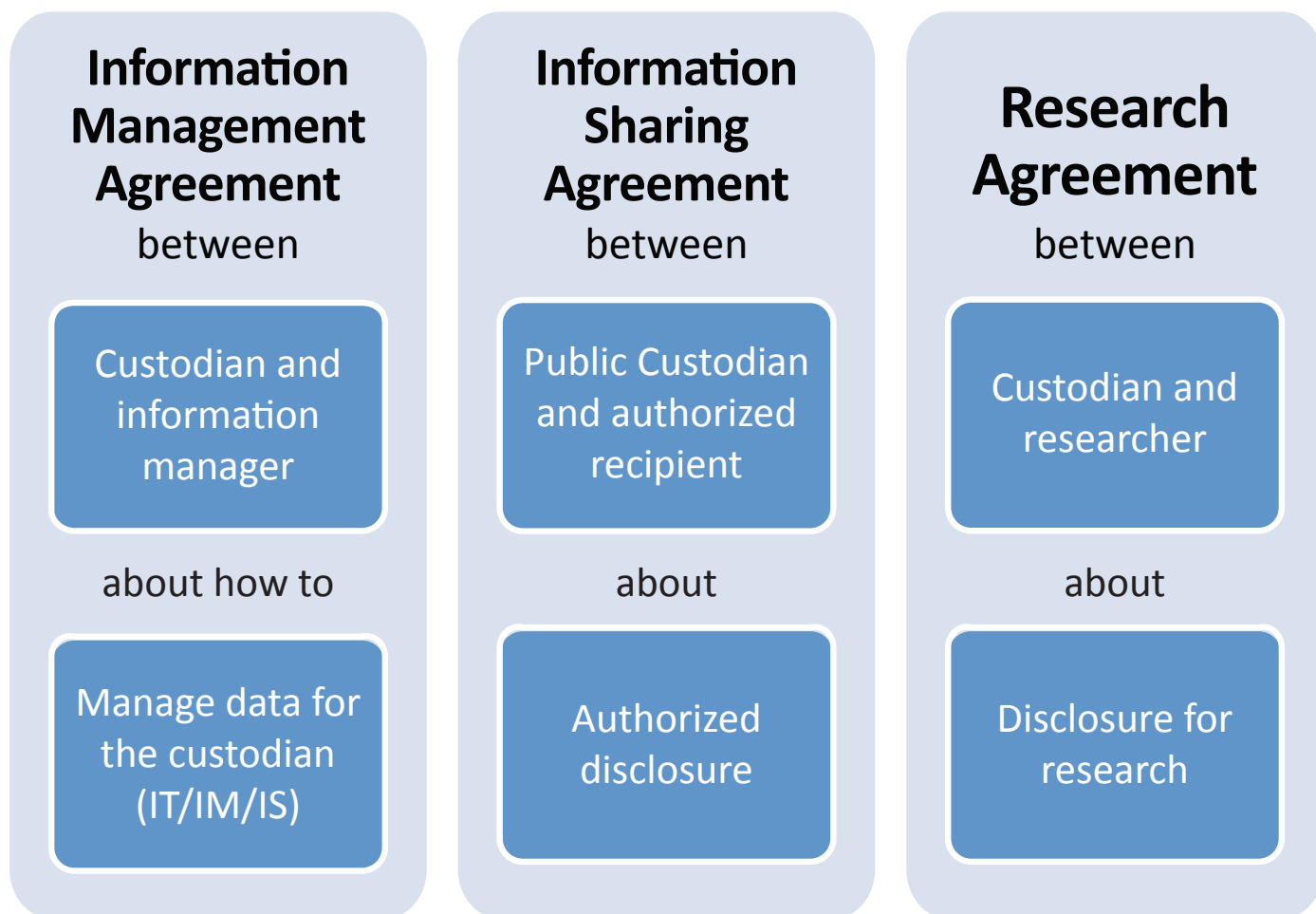
Comparison of Information Management Agreements, Information Sharing Agreements, and Research Agreements

Information management agreements (IMA), information sharing agreements (ISA), and research agreements (RA) all require the custodian to authorize access to patients' personal health information.

Comparison of Information Management Agreements, Information Sharing Agreements, and Research Agreements

Information management agreements (IMA), information sharing agreements (ISA), and research agreements (RA) all require the custodian to authorize access to patients' personal health information.

For more information, see Chapter 8, Information Managers and Information Management Agreements, in the *Health Information Act Guide*, or the HIA.



Chapter 9. Information and Privacy Commissioner – Resources



(For more information about the IPC, see [Chapter 10, Access to and Correction of Personal Health Information](#) and [Chapter 11, Privacy Breach](#).)

Chapter 10. Access to and Correction of Personal Health Information – Resources

Formal Access Request: Suggested Tasks and Timelines

Use this as a worksheet for more complicated access request to record start and stop dates in the access timelines. The worksheet summarizes key steps required to process access requests under the HIA.

Access Request Timelines

Summary of timelines for access requests under the HIA.

Correction Request Timelines

Summary of timelines for correction requests under the HIA.

Access Requests at-a-Glance

Summary of mandatory and discretionary exceptions under the HIA.

Flowcharts

Flowchart diagrams to assist you with

1. **Access to Personal Health Information Process,**
2. **Correction to Personal Health Information Process; and**
3. **Review and Appeal Process under the HIA.**

Formal Access Request: Suggested Tasks and Timelines

A health information custodian will respond to an applicant who makes an access request under section 96 of the Act. The custodian may respond to the applicant earlier than required in the HIA and not later than 30 days after receiving the access request. Custodians may use this as a worksheet for more complicated access request to record start and stop dates in the access timelines. The worksheet summarizes key steps required to process access requests.

Anyone who makes an access request under section 96 of the Act must pay a fee to a health information custodian if the health information custodian estimates that the costs associated with providing access will be more than the amount in the *Health Information Regulations* s.9.

Note: The following access request chart may also be used as a guide for processing correction requests; however, no fees may be charged and the correction must be made on the same day when a response to the request is made.

Calendar Days	Responsible Person / Area	Key Tasks	HIA References
Day 1	Designated contact person or agent (person responsible for release of information)	<p>Step 1. Review request.</p> <p>Confirm that it is an access request under Part 5 of the HIA.</p> <p>Confirm that the request is for records covered by the HIA.</p> <p>Register and log receipt of the request.</p> <p>Acknowledge receipt of the request. (<i>HIA s.101</i>).</p> <p>If the information can be released through a more routine process, advise the applicant of that option.</p> <p>Create request file.</p> <p>If part of the request is deemed to be a request under the <i>Access to Information and Protection of Privacy Act</i> (ATIPP), explain to the applicant how the ATIPP request will be dealt with.</p>	s.96, s.97, s.101, s.104

Calendar Days	Responsible Person / Area	Key Tasks	HIA References
Days 1–10	Designated contact person	<p>Step 2. Request additional information.</p> <p>If processing cannot begin immediately, contact the applicant directly to define or clarify the request.</p> <p>Within 10 days of getting an access request, the custodian must ask the patient for more information if it is necessary to fulfill the request.</p> <p>Requests for large amounts of information can result in significant fees being assessed. Try to narrow the request while still meeting the applicant’s needs.</p> <p>If the request is changed, document the change and send a notice to the applicant.</p> <p>If no additional information is required, go to Step 4.</p>	s.104(2)
Clock stops		<p>Step 3. Wait for further information.</p> <p>Applicant to provide further information to the custodian to clarify the request.</p>	
Days 2–10	Designated contact person or agent (person responsible for release of information)	<p>Step 4. Locate records.</p> <p>Request records from the departments or organizations that are most likely to have them (if applicable). Locate and retrieve the records.</p>	s.104

Calendar Days	Responsible Person / Area	Key Tasks	HIA References
	Transfer to another custodian	<p>Step 5. Transfer request.</p> <p>A health information custodian may transfer an access request or part of an access request to another custodian, if the requested record/part was:</p> <ul style="list-style-type: none"> • made by the other custodian • first collected by the other custodian • in the other custodian's custody <p>The custodian must notify the patient right away when a request is transferred. The notice will state:</p> <ul style="list-style-type: none"> • that the access request has been transferred • the reason for the transfer • the health information custodian to which the access request has been transferred • the patient's right to ask the IPC to review the transfer <p>The custodian receiving the transfer must tell the patient how to get in touch with their designated contact person if he or she has questions.</p>	s.108
Days 2–20	Designated contact person	<p>Step 6. Preliminary review.</p> <p>Prepare records for review and complete the request documentation.</p> <p>List areas searched.</p> <p>List records located.</p> <p>Log staff time spent searching and retrieving records.</p> <p>If necessary, ask the Information and Privacy Commissioner (IPC) for permission to ignore the request. Go to Step 7.</p> <p>Copy and number retrieved records (to make a working copy). Go to Step 8.</p>	s.105, s.129

Calendar Days	Responsible Person / Area	Key Tasks	HIA References
Clock stops	IPC	<p>Step 7. IPC review request to disregard.</p> <p>The clock stops if the custodian asks the IPC to review a request to determine if the custodian can ignore the request.</p> <p>Date stops:</p> <p>Date starts:</p> <p>The clock starts on the day the IPC notifies the custodian of the decision with any delays or extensions otherwise allowed.</p>	s.105, s.129, s.130, s.131
Days 2–20	Designated contact person	<p>Step 8. Extend time limit.</p> <p>If necessary, extend the 30-day time limit by no more than another 30 days. This is allowed if:</p> <ul style="list-style-type: none"> • A large number of records must be reviewed, or • The custodian needs to consult with someone to make sure the applicant has a right to the record. <p>If the time limit is extended, notify the applicant:</p> <ul style="list-style-type: none"> • when they should expect a response • that the time limit is extended • the reason for the extension • when the patient should expect a response • that the patient can ask the IPC to review the time extension <p>Respond to the applicant on or before the end date of the extension.</p>	s.106
Day 1 of custodian extension Clock stops	Designated contact person / staff	<p>Step 9. Request IPC to extend time limit (day 1 of custodian extension).</p> <p>Ask the IPC for further extension if necessary.</p> <p>If the IPC denies the extension, respond to the patient within 30 days of receiving the IPC's decision.</p> <p>Date stops:</p> <p>Date starts:</p>	s.107

Calendar Days	Responsible Person / Area	Key Tasks	HIA References
Day 20	Designated contact person	<p>Step 10. Provide fee estimate to applicant.</p> <p>The estimate of fees and disbursements prepared under this section of the Act must address all applicable fees set out in Part 1 of Schedule B of the <i>Health Information Regulations</i>.</p>	s.104(2) Regs s.10
Clock stops	Designated contact person	<p>Step 11. Wait for applicant approval of fee estimate.</p> <p>Suspend processing until fee estimate approval is received from applicant.</p> <p>Date stops:</p> <p>Date starts:</p>	s.104(2)(b)
Clock stops	Applicant	<p>Step 12. Applicant confirmation.</p> <p>Applicant accepts the fee estimate and asks the designated contact person to proceed with the access request or withdraw the request.</p> <p>If the patient does not respond to a fee estimate or request for more information, the custodian can close the access request after 60 days.</p> <p>Date stops:</p> <p>Date starts:</p>	s.104(2)(b) s.104(5)
Days 20–25	Designated contact person / staff	<p>Step 13. Review responsive records.</p> <p>Complete line-by-line review of the records and consider mandatory and discretionary exceptions. Sever records and indicate the Act section number used to sever the information. (For more information, see “Access Requests at a Glance” in the HIA Guide.)</p> <p>Document exceptions.</p>	
Days 25–29	Designated contact person / staff	<p>Step 14. Make recommendations to custodian.</p> <p>Final analysis of reviews and recommendations.</p> <p>Present final recommendations for the custodian who makes decisions on the access requests.</p>	

Calendar Days	Responsible Person / Area	Key Tasks	HIA References
Day 30	Designated contact person	<p>Step 15. Invoice fees.</p> <p>When the custodian has provided a fee estimate, send the patient an invoice within 10 days after the patient confirms that she or he approves the fee estimate and wants to proceed with the access request.</p>	s.104(3), Regs s.10, Regs s.11
Day 30	Designated contact person / staff	<p>Step 16. Response letter.</p> <p>If access to the record is being given, send a response letter to access request to the applicant. The response letter, including a list of the records the person will receive, will be sent by day 30.</p> <p>If access to the record or part of the record is refused, and the record is not being given out send the applicant a response letter identifying reasons for the refusal.</p>	s.101 s.101(c)
Clock stops	Designated contact person	<p>Step 17. Fees payment.</p> <p>Collect fees owing if applicable. No further processing occurs until fee balance is received.</p> <p>Date stops:</p> <p>Date starts:</p>	
Days 30–60	Designated contact person / staff	<p>Step 18. Release records.</p> <p>Enclose copies of records.</p> <p>The decision to grant access can be at day 30 (or earlier), but there is an additional 30 days available to provide access to the documents/deliver the records.</p>	s.103

Access Request Timelines

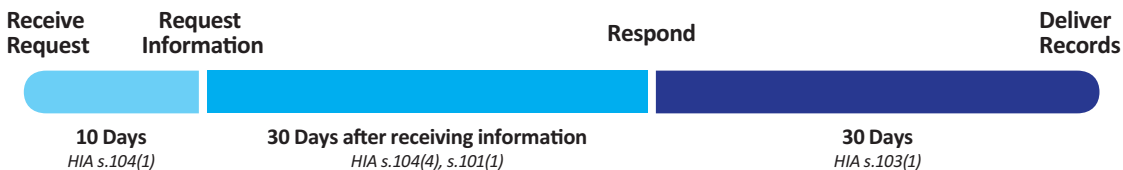
Summary of timelines for access requests.

Access Request Timelines

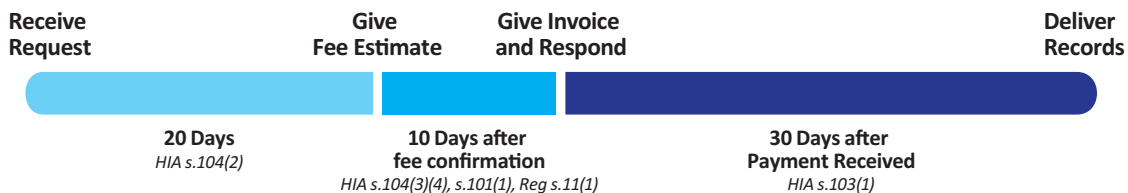
Regular Access Request - (No need for more information; No fees)



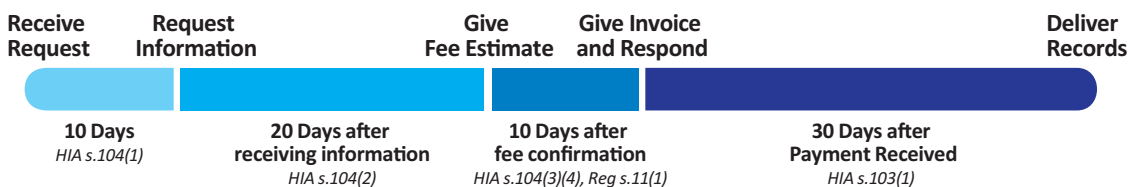
Access Request requiring more information



Access Request requiring fees



Access Request requiring more information and fees



For additional information regarding:
time extensions, see *HIA s.106*
IPC reviews, see *HIA s.106, 107*
transfer of access request to another custodian, see *HIA s.108*

Correction Request Timelines

Summary of timelines for correction requests.

Correction Request Timelines

Regular Correction Request - (No need for more information)



Correction Request requiring more information



Access Requests at-a-Glance

Summary of mandatory and discretionary exceptions under the HIA.

Mandatory Exceptions	
Request	Action
Request for information that involves an invasion of privacy	<p>A request for disclosure of information about another person in the requestor's own chart would invade her or his privacy must be refused. The exception is that a patient who provided the information about the other person can still have access to it.</p> <p><i>(See HIA s.110, Invasion of privacy and exception.)</i></p>
Request for information in a quality assurance activity record	<p>Records created or collected during a quality assurance committee proceeding must not be disclosed. However, if the information is in the patient's chart, the patient can have access to it.</p> <p><i>(See HIA s.111(2), Quality assurance activity.)</i></p>
Request for disclosure of information prohibited by an Act	<p>Disclosure of information that is prohibited by an Act must be refused.</p> <p><i>(See HIA s.112, Disclosure prohibited by Act.)</i></p>
Request for patient information that was provided to or created by the Executive Council or Financial Management Board (FMB)	<p>A request for patient information that was provided to or created by the Executive Council or Financial Management Board (FMB) that would also reveal confidential information of the Council shall be refused. This information may be advice, proposals, and requests for directions, recommendations, analyses, or policy options.</p> <p><i>(See HIA s.117, Executive.)</i></p>

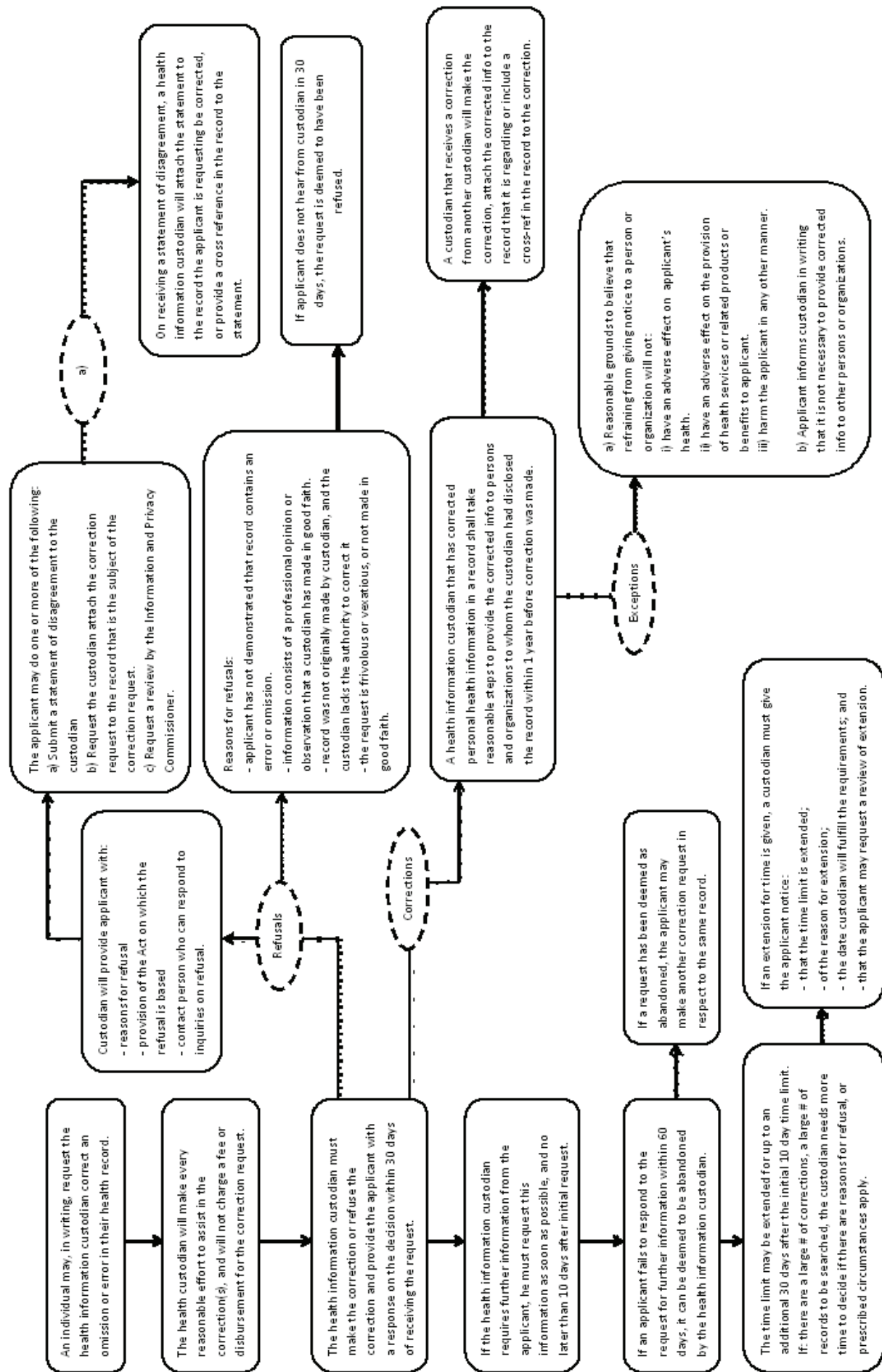
Discretionary Exceptions	
Request	Action
Request for information in quality assurance activity recommendations	<p>Recommendations developed as a result of a quality assurance committee proceeding may be disclosed.</p> <p><i>(See HIA s.111(3), Release of results.)</i></p>

Discretionary Exceptions	
Request	Action
Request for information that may cause harm to the individual making the request	<p>A custodian may refuse to disclose to an applicant information if the disclosure may cause harm to the individual requesting the information. A medical or other expert may determine that a disclosure of personal health information may cause harm to the individual who is the subject of the information.</p> <p><i>(See HIA s.113(1), Disclosure harmful to applicant.)</i></p>
Request for information that may cause harm to any person other than individual making the request	<p>A custodian may refuse to disclose to an applicant information that may cause harm to any individual other than the one making the request. These requests may include situations where the information was provided to the health care provider by another party in confidence and subsequently added to a patient's medical record.</p> <p><i>(See HIA s.113(2), Disclosure harmful to individual or public safety.)</i></p>
Request for information that was collected in confidence	<p>A custodian may refuse to disclose to an applicant information that was collected by the custodian in confidence.</p> <p><i>(See HIA s.114, Information provided in confidence.)</i></p>
Request for information that is subject to legal privilege	<p>A custodian may refuse to disclose to an applicant information that is privileged information between the custodian or agent and a lawyer, or legal advice from a lawyer.</p> <p><i>(See HIA s.115, Privilege.)</i></p>
Request for information that could undermine a law enforcement matter	<p>A custodian may refuse to disclose information to an applicant if the information could prejudice a law enforcement matter, reveal the identity of a confidential source, or reveal a record that has been confiscated from a person.</p> <p><i>(See HIA s.116, Law enforcement matter.)</i></p>
Request for information that is advice from officials	<p>Request for information about internal and health system management advice, analysis, or consultations or advice given to a Minister and Minister's Office may be refused.</p> <p><i>(See HIA s.118(a), Disclosure of advice from officials.)</i></p>

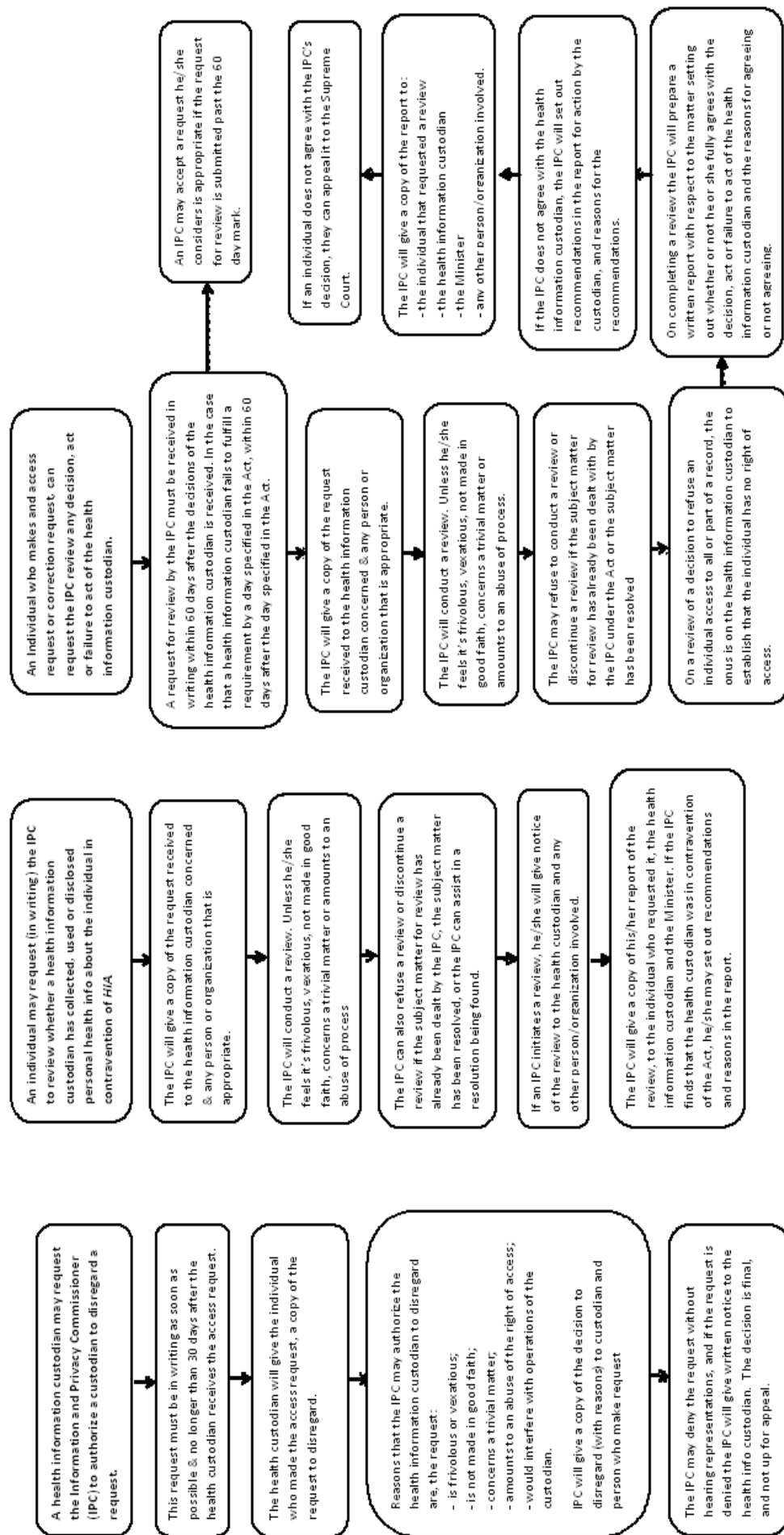
166



Health Information Act: Correction to Personal Health Information Process



Health Information Act: Appeal and Review Process



Chapter 11. Privacy Breach – Resources

These resources are available from DHSS website [health-privacy-protecting-your-health-information](#).

Health Information Regulations - privacy breach reporting requirements.

Privacy Risk Toolkit

Roles and Responsibilities of Designated Contact Persons – Video

What to Do in Case of a Privacy Breach – Video

Chapter 12. Offences and Limitation of Liability– Resources

These resources are available from DHSS website [health-privacy-protecting-your-health-information.](#)

Health Information Act

Health Information Regulations

Answer Key

Test Your Knowledge

Chapter 1. Scope of the Act

1. Examples of personal health information as defined by the HIA:
 - a. Name, date of birth, and address of patient receiving health services
 - b. Progress note on a patient at an outpatient clinic
 - c. Laboratory requisition for a patient
 - f. Pharmacy dispensary patient record
 - g. Medical travel approval, booking, and payment information

Answer d, receipt for crutches purchased at a store, is not correct because *a store is not a custodian*.

Answer e, physician's business card from the health centre, is not correct because *the physician's name is not associated with a health service provided for a specific patient*. ([See Chapter 1, page 10](#))

2. The purposes of the *Health Information Act* are:
 - b. To protect patients' personal health information
 - d. To set rules that custodians must follow when they collect, use, and share patients' personal health information

Answer a, to prevent patients from seeing their medical records, is not correct because *the HIA gives patients the opportunity to access their information*.

Answer c, to make it difficult to share patient information, is not correct because *the HIA authorizes health service providers to share health information for the continuing care and treatment of patients*. ([See Chapter 1, page 6](#))

3. The following must comply with the HIA:
 - a. Department of Health and Social Services
 - b. physicians who own and operate a private medical clinic
 - d. tobacco cessation programs managed by the DHSS and the HSSAs
 - e. medical clinic at an industrial site managed by a physician medical director

In answers a and b, the *DHSS and physicians in private practice are defined as a custodians*. In answer d, *the tobacco cessation programs are managed by health information custodians DHSS and HSSA and involve the use of personal health information*. In answer e, *the medical clinic is managed by a physician (a custodian)*.

Answer c is not correct because *a store is not a custodian*. ([See Chapter 1, page 9](#))

Chapter 2. Custodians and Agents

The following case study applies many of the key concepts in this section. Read the example and answer the questions below.

1. Who is the custodian?
 - *The Health and Social Services Authority is the custodian*. ([See Chapter 2, page 23, 26](#))
2. Who is the agent?
 - *Mary and Pauline are the agents*. ([See Chapter 2, page 23, 26](#))
3. Who is the designated contact person?
 - *Pauline is the authority on the HIA and is the designated contact person*. ([See Chapter 2, page 24, 26](#))
4. Is personal health information collected at the HSSA?
 - *Yes, personal health information is collected at the HSSA*. ([See Chapter 2, page 23, 26](#))
5. Who does the custodian designate to deliver training and monitor compliance?
 - *In this example, Pauline is the designated contact person and is responsible to deliver training and monitor compliance*. ([See Chapter 2, page 26](#))

Chapter 3. Consent

1. Mary sees a physician at HSSA. The physician refers Mary to a specialist physician at another HSSA facility.
 - a. *Implied consent is sufficient*.

Answer b, express consent, is not required because once implied consent has been obtained, *it is not necessary to request it again every time information is shared with other health service providers in order to provide continuing care and treatment*. ([See Chapter 3, page 32](#))

2. Bob's physician writes a referral letter to the private physiotherapist on Bob's behalf and sends the letter by fax. What type of consent is required?
 - a. *Implied consent is sufficient for medically necessary health services*.

Answer b, express consent, is not required. ([See Chapter 3, page 32](#))

3. The elements of valid consent are:

b. Consent of the individual, relate to the information, knowledgeable and not obtained through deception.

Answer b is the most correct.

Answers a and d are not correct because ***a person's email address and information release date are not required in a valid consent.*** ([See Chapter 3, page 31](#))

4. Patients have the right to determine who has access to their personal health information and to set limits on the collection, use, and sharing of that information.

a. true

Answer b, false, is not correct because ***patients have rights to set limits about their personal health information except when required by law.*** ([See Chapter 3, page 35](#))

5. Express consent can be either written or verbal.

a. true

Express consent may be provided in verbal form if the custodian believes that it is not practical for consent to be provided in writing, such as when a patient is unable to write for a reason such as illiteracy or physical disability. ***The custodian must record the verbal express consent in writing*** as soon as possible, including the reason why a written express consent was not possible, and place this document in the patient's file. ([See Chapter 3, page 33](#))

Chapter 4. Collection

1. Who are the people that collect personal health information and have a special responsibility to manage the private information provided to them?

b. custodians

Answer a and c are not correct because ***custodians have a responsibility to manage private information and follow the HIA.*** ([See Chapter 4, page 42](#))

2. It is the gathering, acquiring, receiving, or obtaining of health information from an individual:

b. collection

Answer a and c are not correct because ***gathering, acquiring, receiving, or obtaining of health information is not use or sharing.*** ([See Chapter 4, page 42](#))

3. Who are the people that are authorized to collect or use a patient's health care number:

a. the patient

b. a custodian or the custodian's agent

d. a community pharmacist

Answer c is not correct, ***an adventure tour company is not a custodian.*** A person other than a health information custodian who asks a patient to provide a personal health number must tell the patient why she or he is authorized to have it. ([See Chapter 4, page 44](#))

Chapter 5. Use

1. The following statement is **false**.

A custodian may use personal health information for the following reason:

c. to make money by selling the health information collected

Answer a, b, and d are true. *Custodians may use personal health information to provide health services, to do research, and/or to comply with a law or court order* but not to make money by selling the health information collected. ([See Chapter 5, page 50](#))

2. When can a custodian use personal health information?

d. All of the above.

Answer d is correct because *a custodian can use personal information when:*

- a. The custodian has the patient's consent to use the information.
- b. The use is permitted or required by the HIA or another Act of the NWT or an Act or regulation of Canada.
- c. The HIA or another Act of the NWT or Act or regulation of Canada permits or requires a person or organization to disclose the information to the custodian without the express consent of the individual the information is about. ([See Chapter 5, page 50](#))

3. Custodians may strip and transform personal health information to make it non-identifiable data:

a. true

Answer b, false, is not correct because *custodians may strip and transform personal health information to make it non-identifiable data in accordance with established de-identification procedures that address re-identification risks*. ([See Chapter 5, page 51](#))

4. In the scenario provided, Mr. Tatum's information was used:

c. to comply with a law or court order

Answer a is not correct because *the information is not used for research*.

Answer b is not correct because *no health service provider is being educated*. ([See Chapter 5, page 51](#))

5. Data matching is often used to make sure patient records are complete and for data integrity.

a. true

Answer b, false, is not correct because *custodians may match data from two or more data sources and is often used to make sure patient records are complete and for data integrity by confirming information is added to the correct medical record*. ([See Chapter 5, page 52](#))

Chapter 6. Disclosure

1. When you document a disclosure, you must record:

Answer d, all of the above, is correct because you must record:

- a. what was disclosed, to whom, when, and the purpose of the disclosure
- b. who made the disclosure and the authority to disclose
- c. what format was used to disclose, and when ([See Chapter 6, page 66](#))

2. A good test to assess if you completely documented the disclosure is to

c. Have a co-worker follow your disclosure notation to successfully re-create the same package of information.

Answer a and b are not correct because *the disclosure note should be clearly written with enough detail that someone else can re-create the package of information.* ([See Chapter 6, page 66](#))

3. When in doubt about how to process a request for information:

Answer e, all of the above, is correct to take any of these steps when in doubt about how to process a request for information:

- a. Determine if the individual has provided consent.
- b. Determine if the request relates to a current life threatening circumstance.
- c. Don't disclose.
- d. Ask your supervisor, designated contact person or custodian for assistance. ([See Chapter 6, page 58](#))

4. What is a warrant?

a. A written judicial authorization to search for and collect information or an object

Answer b is not correct because *it is an order.*

Answer c is not correct because *it is a subpoena.* ([See Chapter 6, page 61](#))

5. A health information custodian is told to disclose information to a complaints officer reviewing a complaint against a health professional. This is a mandatory disclosure.

b. false

Answer a, true, is not correct because *this is a discretionary disclosure. Custodians can share personal health information about a patient to an investigator, adjudicator, complaints officer, or board of inquiry investigating a complaint against a health professional.* ([See Chapter 6, page 60](#))

6. A public custodian has a request from a patient to not have their clinic information in the EMR. The public custodian has access to the EMR and regularly puts patient clinic information in the EMR. The public custodian can choose not to put this patient's information in the EMR.

b. false

Answer a, true, is not correct because *the DHSS and the HSSAs must enter personal health information into designated electronic health information systems, such as the electronic medical record (EMR) system.* ([See Chapter 6, page 65](#))

Chapter 7. Disclosure for Research and Research Ethics Committee

1. Researchers may contact patients directly to get consent

b. false

Answer a is not correct because *only custodians may first contact patients and request their express consent*. Patients are not required to join the research study. ([See Chapter 7, page 74](#))

2. A research application was not approved by an REC. The researcher can directly ask a custodian to join a research study.

b. false

Answer a is not correct because *research proposals which include the collection, use or sharing of personal health information held by a custodian must be approved by a REC prior to a researcher asking a custodian for the information*. ([See Chapter 7, page 74](#))

3. A custodian has received an invitation to participate in a research study. What must the researcher provide to the custodian?

b. the license from Aurora Research Institute

c. the research proposal

d. the REC's decision

e. the researcher's resumé

f. any other information the custodian needs about express consent, conditions, or recommendations set by the REC

Answers b, c, d, e and f are correct because *these items are specifically listed in the HIA. A researcher's resume may be included in those additional documents a custodian may request*.

Answer a is not correct. *Researchers should not have a list of patient names; only custodians may make the first contact with patients*. ([See Chapter 7, page 73](#))

4. Which of the following is an agreement between a custodian and a researcher?

c. Research agreement

Answers a and b are not correct. *Information management agreement is between a custodian and information manager. Information sharing agreement is between a public custodian and authorized recipient*. ([See Chapter 7, page 73](#))

Chapter 8. Information Managers and Information Management Agreements

1. Which of the following is an agreement between a custodian and a business or organization to store patients' medical records remotely?

a. information management agreement

Answers b and c are not correct because *b, Information sharing agreement is between a public custodian and authorized recipient and c, research agreement is between a custodian and a researcher.* ([See Chapter 8, page 80](#))

2. A written agreement between a custodian and a business organization must be in place before the custodian can share the information.

a. true

Answer b, false, is not correct because *a custodian and information manager must sign an information management agreement (IMA) before the information manager can begin working.* ([See Chapter 8, page 80](#))

3. In general, an Information Management Agreement is required when:

d. none of the above

Answers a, b, and c are not correct because *an IMA is required for IM/IT/IS services.* ([See Chapter 8, page 80](#))

Chapter 9. Information and Privacy Commissioner

1. IPC stands for:

a. Information and Privacy Commissioner

Answers b and c are not correct. ([See Chapter 9, page 85](#))

2. The IPC is appointed under what Act?

b. Access to Information and Protection of Privacy Act (ATIPP)

Answers a and c are not correct. ([See Chapter 9, page 86](#))

3. The IPC may collect evidence during a review or appeal. The information can be used:

Answer e, all of the above, is correct because *the IPC can use information collected in evidence:*

- a. in the course of a review
- b. in her report
- c. for law enforcement purposes (relating to an offense)
- d. for prosecution, application or appeal

The IPC may also be used for law enforcement purposes (relating to an offense) and for prosecution, application or appeal. ([See Chapter 9, page 87](#))

4. The IPC plays what role under the HIA?

c. An oversight role

Answers a and b are not correct. *The IPC is responsible for promoting compliance with the HIA and for ensuring custodians properly protect patient information and their privacy. The IPC is available to help health information custodians and patients find solutions to privacy issues. (See Chapter 9, page 86)*

Chapter 10. Access to and Correction of Personal Health Information

1. A patient has the right to access his or her personal health information that is under the custody or control of the custodian.

a. true

Answer b, false, is not correct because *under HIA s.94, the patient has the right to access any record containing personal health information about him or her. (See Chapter 10, page 94)*

2. Julia moved recently. On her next visit to the doctor she asks that her address be changed in her medical record. Can she do that?

a. Yes.

Answer b, no, is not correct because *a patient can make an informal correction request when they are receiving health services. The custodian make every reasonable effort to respond accurately and quickly. (See Chapter 10, page 101)*

3. A health information custodian has to respond to an access request in writing no later than how many days after receiving the request?

c. 30 days

Answer a and b, is not correct because *a custodian shall give a response to an access request no later than 30 days after receiving it. (See Chapter 10, page 95)*

4. George has been diagnosed with schizophrenia. His doctor asked his mother about his behaviour. George's mother responded that her son has been angry, confused, and paranoid for the past six months. After being discharged, George asks to see his medical record. Should he have access to his information?

c. Yes.

Answers a and b are not correct because *George should have access, but the information his mother gave in confidence should be severed first.*

Under section 114 of the Act, a custodian must not disclose any information that could identify another person who gave that information in confidence. *(See Chapter 10, page 96)*

5. A custodian may refuse to make a requested correction to a record if:

d. all of the above.

Answer d, all of the above, is correct because *a custodian may refuse to make a requested correction to information in a record if the patient has not proved there is an error, the information is a professional opinion, or the request is frivolous or made in bad faith. (See Chapter 10, page 103)*

6. If a report by the IPC includes recommendations for action by a health information custodian, the custodian can accept the recommendations without taking any additional actions.

b. False

Answer a, true, is not correct because *within 30 days after getting the IPC's recommendations, the custodian must tell the IPC, the person who requested the review, and the Minister of Health and Social Services the custodian's decision as to whether it accepts any or all of the IPC's recommendations*. If the custodian decides to accept any or all of the IPC's recommendations, the custodian must implement the recommendations within 45 days of its decision. ([See Chapter 10, page 99](#))

Chapter 11. Privacy Breaches

1. Privacy breaches include:

e. any of the above

Answer e, any of the above, is correct because *a privacy breach happens when any of these events happen – unauthorized collection, unauthorized use, unauthorized sharing, or loss of personal health information*. ([See Chapter 11, page 109](#))

2. Which of the following are examples of a privacy breach?

a. agent discloses the health care number of a patient to the patient's school without the express consent of the patient

b. looking up your friend's birth date on the EMPI

c. patient's referral letter is faxed to a store instead of the family physician's office

d. paper with patient information is put in the garbage instead of secure shredding

Answers e and f are authorized uses of personal health information ([See Chapter 11, page 110](#))

3. What are custodians' roles when preventing or responding to a privacy breach?

a. Custodians are responsible for notifying a patient whose personal health information has been breached.

c. Custodians should develop and implement procedures that effectively prevent and manage privacy breaches.

d. Custodians must consider appropriate discipline in the event of a privacy breach.

Answer a, c, and d are correct because *if a privacy breach occurs, custodians are responsible for notifying a patient whose personal health information has been breached, developing and implementing procedures, and considering appropriate discipline*. They must also gather evidence when a privacy breach occurs. ([See Chapter 11, page 112](#))

4. An individual can contact the IPC and request a review of a potential breach.

a. true

Answer b, false, is not correct because *a patient who thinks a custodian has collected, used, or disclosed his or her personal health information in contravention of the HIA may ask the IPC for a review*. ([See Chapter 11, page 114](#))

Chapter 12. Offences and Limitation of Liability

1. Which of the following individuals are immune from liability if they act in good faith?

Answer d, all of the above, is correct.

As long as their actions were in good faith, custodians, the IPC, and providers of information have immunity from liability. ([See Chapter 12, page 122](#))

2. Interfering or misleading the IPC, custodians, or Supreme Court is an offence under the Act.

a. true

Answer b, false, is not correct because *interfering or misleading the IPC, custodians, or Supreme Court is considered obstruction and is prohibited under the Act.* ([See Chapter 12, page 122](#))

Links to the Act

The *Health Information Act Guide* contains information related to many parts of the HIA. When you need additional information about a particular section of the Act, refer to this table to locate relevant discussions in the Guide.

Part 1. How the Act Applies

Act	HIA Guide
s.1	Chapter 1, Scope of the Act
s.2	Chapter 1, Scope of the Act
s.3	Chapter 1, Scope of the Act
s.4	Chapter 1, Scope of the Act
s.5	Chapter 1, Scope of the Act
s.6	Chapter 1, Scope of the Act

Part 2. Roles and Responsibilities

Health Information Custodians

Act	HIA Guide
s.7	Chapter 1, Scope of the Act
s.8	Chapter 2, Custodians and Agents Chapter 11, Privacy Breach

Agents

Act	HIA Guide
s.9	Chapter 2, Custodians and Agents Chapter 11, Privacy Breach
s.10	Chapter 2, Custodians and Agents Chapter 11, Privacy Breach
s.11	Chapter 2, Custodians and Agents Chapter 11, Privacy Breach

Contact Persons

Act	HIA Guide
s.12	Chapter 2, Custodians and Agents Chapter 10, Access and Correction Chapter 11, Privacy Breach

Information Managers and Information Management Agreements

Act	HIA Guide
s.13	Chapter 2, Custodians and Agents Chapter 8, Information Managers and Information Management Agreements

Part 3. Consent and Substitute Decision Makers

Consent

Act	HIA Guide
s.14	Chapter 3, Consent
s.15	Chapter 3, Consent
s.16	Chapter 3, Consent
s.17	Chapter 3, Consent
s.18	Chapter 3, Consent
s.19	Chapter 3, Consent
s.20	Chapter 3, Consent
s.21	Chapter 3, Consent
s.22	Chapter 3, Consent
s.23	Chapter 3, Consent
s.24	Chapter 3, Consent

Substitute Decision-Makers

Act	HIA Guide
s.25	Chapter 3, Consent
s.26	Chapter 3, Consent

Part 4. Collection, Use, Disclosure and Protection of Personal Health Information

General Requirements Collection, Use and Disclosure

Act	HIA Guide
s.27	Chapter 4, Collection Chapter 5, Use Chapter 6, Disclosure Chapter 7, Disclosure for Research and Research Ethics Committee
s.28	Chapter 4, Collection Chapter 5, Use Chapter 6, Disclosure Chapter 7, Disclosure for Research and Research Ethics Committee

Collection of Personal Health Information

Act	HIA Guide
s.29	Chapter 4, Collection
s.30	Chapter 4, Collection
s.31	Chapter 4, Collection
s.32	Chapter 4, Collection
s.33	Chapter 4, Collection

Use of Personal Health Information

Act	HIA Guide
s.34	Chapter 5, Use
s.35	Chapter 5, Use
s.36	Chapter 5, Use
s.37	Chapter 5, Use

Disclosure of Personal Health Information

Act	HIA Guide
s.38	Chapter 6, Disclosure
s.39	Chapter 6, Disclosure
s.40	Chapter 6, Disclosure
s.41	Chapter 6, Disclosure
s.42	Chapter 6, Disclosure
s.43	Chapter 6, Disclosure
s.44	Chapter 6, Disclosure
s.45	Chapter 6, Disclosure
s.46	Chapter 6, Disclosure
s.47	Chapter 6, Disclosure
s.48	Chapter 6, Disclosure
s.49	Chapter 6, Disclosure
s.50	Chapter 6, Disclosure
s.51	Chapter 6, Disclosure
s.52	Chapter 6, Disclosure
s.53	Chapter 6, Disclosure
s.54	Chapter 6, Disclosure
s.55	Chapter 6, Disclosure
s.56	Chapter 6, Disclosure
s.57	Chapter 6, Disclosure
s.58	Chapter 6, Disclosure
s.59	Chapter 6, Disclosure
s.60	Chapter 6, Disclosure
s.61	Chapter 6, Disclosure
s.62	Chapter 6, Disclosure
s.63	Chapter 6, Disclosure
s.64	Chapter 6, Disclosure
s.65	Chapter 6, Disclosure
s.66	Chapter 6, Disclosure

Collection, Use and Disclosure of Personal Health Information for Research Purposes

Act	HIA Guide
s.67	Chapter 7, Disclosure for Research and Research Ethics Committee
s.68	Chapter 7, Disclosure for Research and Research Ethics Committee
s.69	Chapter 7, Disclosure for Research and Research Ethics Committee
s.70	Chapter 7, Disclosure for Research and Research Ethics Committee
s.71	Chapter 7, Disclosure for Research and Research Ethics Committee

Act	HIA Guide
s.72	Chapter 7, Disclosure for Research and Research Ethics Committee
s.73	Chapter 7, Disclosure for Research and Research Ethics Committee
s.74	Chapter 7, Disclosure for Research and Research Ethics Committee
s.75	Chapter 7, Disclosure for Research and Research Ethics Committee
s.76	Chapter 7, Disclosure for Research and Research Ethics Committee
s.77	Chapter 7, Disclosure for Research and Research Ethics Committee
s.78	Chapter 7, Disclosure for Research and Research Ethics Committee
s.79	Chapter 7, Disclosure for Research and Research Ethics Committee
s.80	Chapter 7, Disclosure for Research and Research Ethics Committee
s.81	Chapter 7, Disclosure for Research and Research Ethics Committee
s.82	Chapter 7, Disclosure for Research and Research Ethics Committee
s.83	Chapter 7, Disclosure for Research and Research Ethics Committee

Record of Disclosure

Act	HIA Guide
s.84	Chapter 6, Disclosure Chapter 10, Access and Correction of Personal Health Information

Protection of Personal Health Information

Act	HIA Guide
s.85	Chapter 2, Custodians and Agents Chapter 11, Privacy Breach
s.86	Chapter 2, Custodians and Agents Chapter 11, Privacy Breach
s.87	Chapter 11, Privacy Breach
s.88	Chapter 2, Custodians and Agents Chapter 4, Collection Chapter 5, Use Chapter 6, Disclosure Chapter 7, Disclosure for Research and Research Ethics Committee
s.89	Chapter 2, Custodians and Agents Chapter 11, Privacy Breach

Part 5. Access to and Correction of Personal Health Information

Interpretation and Application

Act	HIA Guide
s.90	Chapter 10, Access to and Correction of Personal Health Information
s.91	Chapter 10, Access to and Correction of Personal Health Information
s.92	Chapter 10, Access to and Correction of Personal Health Information
s.93	Chapter 10, Access to and Correction of Personal Health Information

Access to Personal Health Information

Act	HIA Guide
s.94	Chapter 10, Access to and Correction of Personal Health Information
s.95	Chapter 10, Access to and Correction of Personal Health Information
s.96	Chapter 10, Access to and Correction of Personal Health Information
s.97	Chapter 10, Access to and Correction of Personal Health Information
s.98	Chapter 10, Access to and Correction of Personal Health Information
s.99	Chapter 10, Access to and Correction of Personal Health Information
s.100	Chapter 10, Access to and Correction of Personal Health Information
s.101	Chapter 10, Access to and Correction of Personal Health Information
s.102	Chapter 10, Access to and Correction of Personal Health Information
s.103	Chapter 10, Access to and Correction of Personal Health Information
s.104	Chapter 10, Access to and Correction of Personal Health Information
s.105	Chapter 10, Access to and Correction of Personal Health Information
s.106	Chapter 6, Disclosure and Protection of Personal Information Chapter 10, Access to and Correction of Personal Health Information
s.107	Chapter 10, Access to and Correction of Personal Health Information
s.108	Chapter 10, Access to and Correction of Personal Health Information
s.109	Chapter 10, Access to and Correction of Personal Health Information

Exceptions to Providing Access

Act	HIA Guide
s.110	Chapter 10, Access to and Correction of Personal Health Information
s.111	Chapter 10, Access to and Correction of Personal Health Information
s.112	Chapter 10, Access to and Correction of Personal Health Information
s.113	Chapter 10, Access to and Correction of Personal Health Information
s.114	Chapter 10, Access to and Correction of Personal Health Information
s.115	Chapter 10, Access to and Correction of Personal Health Information
s.116	Chapter 10, Access to and Correction of Personal Health Information

Act	HIA Guide
s.117	Chapter 10, Access to and Correction of Personal Health Information
s.118	Chapter 10, Access to and Correction of Personal Health Information

Correction of Personal Health Information

Act	HIA Guide
s.119	Chapter 10, Access to and Correction of Personal Health Information
s.120	Chapter 10, Access to and Correction of Personal Health Information
s.121	Chapter 10, Access to and Correction of Personal Health Information
s.122	Chapter 10, Access to and Correction of Personal Health Information
s.123	Chapter 10, Access to and Correction of Personal Health Information
s.124	Chapter 10, Access to and Correction of Personal Health Information
s.125	Chapter 10, Access to and Correction of Personal Health Information
s.126	Chapter 10, Access to and Correction of Personal Health Information
s.127	Chapter 10, Access to and Correction of Personal Health Information
s.128	Chapter 10, Access to and Correction of Personal Health Information

Part 6. Review and Appeal

Request for Authorization to Disregard Access Request

Act	HIA Guide
s.129	Chapter 10, Access to and Correction of Personal Health Information
s.130	Chapter 10, Access to and Correction of Personal Health Information
s.131	Chapter 10, Access to and Correction of Personal Health Information

Request for Extension of Time Limit for Responding to Access Requests and Correction Requests

Act	HIA Guide
s.132	Chapter 10, Access to and Correction of Personal Health Information
s.133	Chapter 10, Access to and Correction of Personal Health Information

Reviews Relating to Collection, Use and Disclosure of Personal Health Information

Act	HIA Guide
s.134	Chapter 11, Privacy Breach
s.135	Chapter 11, Privacy Breach
s.136	Chapter 11, Privacy Breach
s.137	Chapter 11, Privacy Breach
s.138	Chapter 11, Privacy Breach
s.139	Chapter 11, Privacy Breach
s.140	Chapter 11, Privacy Breach

Request for Review: Access Request and Correction Request

Act	HIA Guide
s.141	Chapter 10, Access to and Correction of Personal Health Information
s.142	Chapter 10, Access to and Correction of Personal Health Information
s.143	Chapter 10, Access to and Correction of Personal Health Information
s.144	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.145	Chapter 10, Access to and Correction of Personal Health Information
s.146	Chapter 10, Access to and Correction of Personal Health Information
s.147	Chapter 10, Access to and Correction of Personal Health Information

Procedure and Evidence on Review

Act	HIA Guide
s.148	Chapter 9, Information and Privacy Commissioner
s.149	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.150	Chapter 9, Information and Privacy Commissioner
s.151	Chapter 9, Information and Privacy Commissioner
s.152	Chapter 9, Information and Privacy Commissioner
s.153	Chapter 9, Information and Privacy Commissioner
s.154	Chapter 9, Information and Privacy Commissioner
s.155	Chapter 9, Information and Privacy Commissioner

Decision by Custodian

Act	HIA Guide
s.156	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.157	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.158	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach

Appeal to Supreme Court

Act	HIA Guide
s.159	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.160	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.161	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.162	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.163	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.164	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.165	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach
s.166	Chapter 10, Access to and Correction of Personal Health Information
s.167	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach

Part 7. Information and Privacy Commissioner

Administration

Act	HIA Guide
s.168	Chapter 9, Information and Privacy Commissioner
s.169	Chapter 9, Information and Privacy Commissioner
s.170	Chapter 9, Information and Privacy Commissioner
s.171	Chapter 9, Information and Privacy Commissioner
s.172	Chapter 9, Information and Privacy Commissioner
s.173	Chapter 9, Information and Privacy Commissioner

Appeal to Supreme Court

Act	HIA Guide
s.174	Chapter 9, Information and Privacy Commissioner
s.175	Chapter 9, Information and Privacy Commissioner Chapter 11, Privacy Breach
s.176	Chapter 9, Information and Privacy Commissioner

Powers and Duties of the Information and Privacy Commissioner

Act	HIA Guide
s.174	Chapter 9, Information and Privacy Commissioner
s.175	Chapter 9, Information and Privacy Commissioner Chapter 11, Privacy Breach
s.176	Chapter 9, Information and Privacy Commissioner

Public Register

Act	HIA Guide
s.177	Chapter 9, Information and Privacy Commissioner

Restrictions on Disclosure

Act	HIA Guide
s.178	Chapter 9, Information and Privacy Commissioner
s.179	Chapter 9, Information and Privacy Commissioner

Part 8. General

Limitation of Liability

Act	HIA Guide
s.180	Chapter 12, Offences and Limitation of Liability
s.181	Chapter 12, Offences and Limitation of Liability
s.182	Chapter 12, Offences and Limitation of Liability
s.183	Chapter 12, Offences and Limitation of Liability

Notice

Act	HIA Guide
s.184	Chapter 9, Information and Privacy Commissioner Chapter 10 Access to and Correction of Personal Health Information Chapter 11, Privacy Breach

Offence and Punishment

Act	HIA Guide
s.185	Chapter 12, Offences and Limitation of Liability
s.186	Chapter 12, Offences and Limitation of Liability
s.187	Chapter 12, Offences and Limitation of Liability
s.188	Chapter 12, Offences and Limitation of Liability
s.189	Chapter 12, Offences and Limitation of Liability
s.190	Chapter 12, Offences and Limitation of Liability
s.191	Chapter 12, Offences and Limitation of Liability
s.192	Chapter 12, Offences and Limitation of Liability
s.193	Chapter 12, Offences and Limitation of Liability
s.194	Chapter 12, Offences and Limitation of Liability

Regulation

Act	HIA Guide
s.195	N/A

Review of Act by Minister

Act	HIA Guide
s.195.1	N/A

Transitional

Act	HIA Guide
s.196	Chapter 5, Use Chapter 6, Disclosure Chapter 7, Disclosure for Research and Research Ethics Committee
s.197	Chapter 10, Access to and Correction of Personal Health Information Chapter 11, Privacy Breach

Consequential Amendments

Act	HIA Guide
s.198	Chapter 1, Scope of Act, hierarchy
s.199	Chapter 1, Scope of Act, hierarchy
s.200	Chapter 1, Scope of Act, hierarchy
s.201	Chapter 1, Scope of Act, hierarchy
s.202	Chapter 1, Scope of Act, hierarchy
s.203	Chapter 1, Scope of Act, hierarchy
s.204	Chapter 1, Scope of Act, hierarchy
s.205	Chapter 1, Scope of Act, hierarchy
s.206	Chapter 1, Scope of Act, hierarchy
s.207	Chapter 1, Scope of Act, hierarchy

Commencement

Act	HIA Guide
s.208	N/A

Index

A

access request 92
definition 6
disregard 97
exceptions to 93
exceptions, discretionary 93
exceptions, mandatory 93
request timelines 97, 156, 162
transfer 95
Access to Information and Protection of Privacy Act (ATIPP) 11, 13
addiction services 10
administrative safeguards.
 See safeguards
agent 9
definition 7
alternative dispute resolution 87,
 99, 103, 114
appeal 100, 105, 116
Aurora College Research Ethics
 Committee 72

B

breach. *See* privacy breach

C

collect
definition 7
consent
conditions 35
withdrawal 36
contact person 21, 24
definition 7
correction request 101
definition 7
request timelines 101, 163
counselling 10
court order 51
custodian.
 See health information
 custodian
definition 7

D

data matching 52
deceased 60
de-identification 51
disclose, disclosure 58, 94
definition 7
discretionary 58
for research 75
mandatory 58, 59, 64
note 66
duty to assist 22, 94, 101

E

electronic health information
systems 65
electronic medical record (EMR) 65,
 92
express consent 33, 72, 73, 74
express instructions 33, 35, 59
extra-territorial research ethics
committee 73
definition 7

F

fee
access requests 96
estimate 96
invoice 97
research 75
schedule 96
fines. *See* offence

H

Health Information Act (HIA) 5
purpose 6
health information custodian
definition 7
roles and responsibilities 20
Health Information Regulations 5, 6

health service
definition 7
health service provider
definition 7
hierarchies of privacy rules 13
human resources and employee
records 11

I

identity authentication 32, 95, 101
implied consent 32
individual
definition 7
Information and Privacy
Commissioner (IPC) 85, 92,
 114
definition 7
information management agreement
 (IMA) 80
information manager 80
definition 8
information sharing agreement
 (ISA) 64, 81
invasion of privacy 93
investigate 112
invoice. *See* fee

K

knowledgeable consent 31, 32

L

legal proceeding 61
limitation of liability 122

M

mandatory exception 93
mature minor 30, 59
mental health services 10

N

non-identifiable 50, 51
non-identifying 11
notice
 of collection 21, 31, 43
 to applicant
 permission to disregard 95
 to researcher 73

O

offence 112, 122
order 61

P

patient identifiers 43, 95
patients' rights 6, 101
personal directive 30
personal health information 6, 10
 definition 8
 disclosure 60
 protection 20
personal health number 44, 52
*Personal Information Protection and
 Electronic Documents Act
 (PIPEDA)* 11, 14
photo ID 32, 43
physical safeguards. *See* safeguards
policies and procedures 20, 23, 80
prescription monitoring
 program 36, 65
privacy breach 109
privacy impact assessment
 (PIA) 86, 111
 definition 8
privacy principles 6, 42, 50, 58
private custodian 9, 14
public custodian 8, 13
 definition 9
public health 32, 52, 64
public register 86

Q

quality assurance 50, 61, 93

R

record
 definition 8
recording device 44
record of activity 66, 92
regulation.
 See Health Information
 Regulations
research
 agreement (RA) 73
 application 72
 assessment 72
 definition 8
 disclosure 75
 fee 75
 notice 73
 proposal 72
 request 73
 research ethics committee
 (REC) 71, 72
researcher
 definition 8
research ethics committee
 definition 8
right not to consent 32

S

safeguards 20, 80
 administrative 20, 80, 110
 physical 20, 80, 110
 technical 20, 80, 110
severed 13
subpoena 61
subpoena duces tecum 61
substitute decision-maker 30, 43, 92
 definition 8
Supreme Court 100, 105
 appeal 116

T

technical safeguards.
 See safeguards
transfer an access request.
 See also access request: transfer

U

use 50
 authority to use 50
 definition 8
 secondary 50, 58

V

valid consent 31

W

warrant 61
withdrawal of consent.
 See consent: withdrawal
written express consent 34



Kĩspin ki nitawihtĩn ā nĩhiyawihk ōma ācimōwin, tipwēsinēn.

Cree

ᖃerihł'ís dēne sūliné yati t'a huts'elkēr xa beyéyati theᖅ ᖃat'e, nuwe ts'ēn yółti.

Chipewyan

If you would like this information in another official language, call us.

English

Si vous voulez ces renseignements en français, contactez-nous.

Français

Jii gwandak izhii ginjik vat'atr'ijahch'uu zhĩt yinothan jì', diits'àt ginohknì.

Gwich'in

Hapkua titiqqat pijumagupkit Inuinnaqtun, uvaptinnut hivajarlutit.

Inuinnaqtun

ᑕᖅᑭ ᑎᑎᖅᑕ ᐱᐸᐱᐱᐸ ᐃᖅᑎᑕᖅᑭᐱᑕᑎᖅ, ᐃᐸᐸᑎᖅᑕ ᐃᖅᑕ ᐸᖅᑕᑎᑕ.

Inuktitut

UVANITTUAQ ILITCHURISUKUPKU INUVIALUKTUN, QUQUAQLUTA.

Inuvialuktun

K'éhshó got'ine xədá k'é hederi ᖃedĩhtl'é yeriniwē nídé dúle.

North Slavey

Edi gondı dehgéh got'ie zhatié k'ée edatł'éh enahddhę nide.

South Slavey

Tłıchọ yati k'èè dè wegodiı wek'èhoızo nęęwọ dè, gots'ò goahde.

Tłıchọ

1-867-767-9052, ext. 49045



Health Information Act Guide