



Health and Community Services

**The *Personal Health Information Act*
Facilitated Education Program**

**Facilitator Manual
(Full-Day)**

Version:
Date:

1.0
September, 2010

WARNING AND DISCLAIMER

These educational materials have been prepared by the Department of Health and Community Services as a general guide to assist custodians of personal health information to meet their obligations under Newfoundland and Labrador's *Personal Health Information Act*.

- These materials are designed to assist in complying with the law and meeting the changing expectations of patients and the public.
- The resource materials provided herein are for general information purposes only.
- These materials reflect interpretations and practices regarded as valid when it was published based on information available at that time.
- These materials are not intended, and should not be construed, as legal or professional advice or opinion.
- Custodians concerned about the applicability of privacy legislation to their activities are advised to seek legal or professional advice based on their particular circumstances.

This is the first edition of the PHIA Facilitated Education Program; a second edition may be published in due course.

ACKNOWLEDGEMENT

The PHIA Facilitated Education Program was prepared by the Department of Health and Community Services with the assistance of several stakeholders in the province's health and community services sector. The Department would like to thank the members of the PHIA Provincial Implementation Steering Committee, the PHIA Education Materials Working Group and the Newfoundland and Labrador Office of the Information and Privacy Commissioner for their assistance in preparing these materials.

TABLE OF CONTENTS

Section I: Introduction	1
Section II: Adult Learning	4
Section III: Agenda for Facilitators	7
Section IV. Education Session	8
A: Session Overview & Introductions	8
B: Assessment	10
C: Personal Health Information Act Overview Part One	11
C: Personal Health Information Act Overview Part Two	22
D: Facilitated Discussion	29
E: Small Group Discussion (Scenarios)	31
F: PHIA Resources	36
G: Implementing PHIA in Your Organization	39
H: Closing And Evaluation (15 Minutes)	43

SECTION I: INTRODUCTION

In the spring of 2008, the *Personal Health Information Act* (PHIA) was passed by the Newfoundland and Labrador House of Assembly. The Act applies to both public- and private-sector custodians of personal health information, and establishes rules relating to the collection, use and disclosure of such information; the Act also provides individuals with the right to access and to request correction of their own personal health information.

The Act is available on the Government of Newfoundland and Labrador's website at:

<http://www.assembly.nl.ca/legislation/sr/statutes/p07-01.htm>.

(Please note that the copy of the Act and regulations made available in this policy development manual were prepared by the Office of the Legislative Counsel. As they are not published by the Queen's Printer they are not an official version of the laws of the Province. You should contact the Queen's Printer to obtain the official statement of the law.)

The purposes of the *Personal Health Information Act*, as defined in the Act, are as follows:

- *To establish rules for the collection, use and disclosure of personal health information that protect the confidentiality of that information and the privacy of individuals with respect to that information;*
- *To provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in this Act;*
- *To provide individuals with a right to require the correction or amendment of personal health information about themselves, subject to limited and specific exceptions set out in this Act;*
- *To establish mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control;*
- *To provide for an independent review of decisions and resolution of complaints with respect to personal health information in the custody or control of custodians; and*
- *To establish measures to promote the compliance with this Act by persons having the custody or control of personal health information.*

NOTE: This learning package has been developed to provide you with tools to facilitate face-to-face education to help you and/or your employees meet the legal obligations for the protection of personal health information. In the facilitator's binder, you will find all the tools and information needed to deliver this session. We have provided you with the following:

- A guide to organizing and facilitating sessions
- PowerPoint Slide Deck
- A glossary
- Evaluation form
- Participant Certificate of Attendance
- Participant's Workbook & Handouts

1.1 Learning objectives

This session has been designed to provide staff with an overview of the *Personal Health Information Act* as well as an opportunity to think about situations in which health information is collected, used, stored, disclosed and protected. In addition, staff may also participate in PHIA's on-line training, a series of web-based learning modules, to become aware of their responsibilities and obligations under the Act depending on the role they perform for their employer.

The goal of the session is to provide participants with the information and context to make good decisions regarding the collection, use, and protection of personal health information. At the end of the session, participants will be able to

- *Demonstrate their understanding of the legislation's requirements for the collection, use, and protection of personal health information*
- *Apply the information acquired to appropriate examples relating to the collection, use, and protection of personal health information*
- *Incorporate best practices for the protection of personal health information in their job and in their workplace*
- *Contribute positively to the creation of a culture of privacy in their workplace.*

The session is designed to

- *make participants **aware** of the key concepts represented in the Act*
- *help them **understand** the importance of personal information protection and*
- *support **action** such as creating a culture of privacy in their organization through the implementation of best practices in their work as appropriate for the continued protection of personal health information*

1.2 Facilitator competencies

To deliver this presentation, you should know and be able to demonstrate the following:

- Familiarity with the purposes, principles and concepts incorporated in the *Personal Health Information Act*
- Understanding of the roles and responsibilities (obligations) custodians and others have with respect to implementing the Act
- Confidence when explaining the importance of meeting the organization's policies which guide the implementation of the Act
- Ability to define terms and approaches as used in the act for the participants as required or direct them to additional information resources as needed and appropriate

In future, the personal health information custodian may offer other sessions as part of their responsibility for ongoing education related to changes in policy, regulations or future legislative amendments.

Note: These and other terms such as circle of care and contact person are defined in the glossary as they have specific meanings with respect to the legislation.

1.3 Purpose of the Facilitator's Guide

This guide has been prepared to help you facilitate a learning session of a full-day (six hours), and here you will learn:

- How to use the guide,
- How to identify what learning outcomes, activities and resources you can use to achieve the goal of understanding your responsibilities under the *Personal Health Information Act* and
- Helpful tips on evaluation processes you can take to ensure the participants have acquired the knowledge they need about PHIA to do their jobs well.

1.4 How to use these materials

This guide has been developed to help you deliver education sessions to staff to help them understand their responsibilities with respect to the Personal Health Information Act. While the primary focus is to prepare your audience for the first phase of the Act's implementation, you may also find it helpful to adapt material later on for other occasions. The Guide offers:

- information on adult learning
- organizing and facilitating sessions
- a detailed outline with accompanying notes to help you deliver the session
- supplementary material

1.5 Facilitator's role

Facilitators are key to successful workshops and learning sessions. Your role is to manage the learning environment so participants feel they have benefited from participating in the session. This means both the session and the space you use encourage learning and sharing among participants.

As the Act is implemented, people at all levels, both in the community and in the health system, will become more comfortable with its provisions. This session introduces the key highlights of the new Act, discusses the responsibilities you have for protecting personal information, and creates an opportunity to discuss the changes in a positive learning environment.

As the facilitator, you are responsible for presenting the information provided. If you are unable to answer a question, make a note of it and the participant for later follow up. In fact, you may find it helpful to post a flipchart sheet for that very purpose.

SECTION II. ADULT LEARNING

You may find it helpful to keep the following in mind as you prepare for your sessions. Adults learn in different ways so we have developed the content of these education sessions to use different methods to teach you and/or your employees about the *Personal Health Information Act*. The key adult education learning principles are¹:

- Adults are *autonomous* and *self-directed*. This means that the facilitators involve participants in the learning process and guide participants to their own knowledge rather than merely supplying them with facts in a lecture format.
- Adults have *life experiences* and *knowledge* that may include work-related activities, family responsibilities, and previous education. Successful learning environments connect to this knowledge/experience base.
- Adults are *goal-oriented*. Adults appreciate an educational program that is organized and has clearly defined elements and goals.
- Adults are *relevancy-oriented*. They must see a reason for learning something. Learning has to be applicable to their work or other responsibilities to be of value to them.
- Adults are *practical*. They focus on the aspects that will be most useful in their daily work; they may not necessarily be interested in knowledge for its own sake. Community advocates are busy with job responsibilities, family members are concerned with the demands of caring for their loved ones, and policy makers are focused on their area's accountabilities.
- Regardless of age and perspective, all learners need to be shown *respect*. Facilitators must recognize how much people will bring to the sessions and the facilitator's guides will include suggestions and recommendations on how best to achieve this.

2.1 Some thoughts on group process

Facilitation is managing the conversation between different parties in a structured environment. As facilitator, you are the group's guide; your role is to help direct the conversation in a specific direction or to lead the participants through purposeful learning.

Sometimes the participants may challenge your goals for the session. As the facilitator, you will encounter questions and you will sometimes have to deal with challenges in your sessions. Most questions can be grouped into the following categories:

- 1) **Process** – How will issues, processes, programs etc be implemented?
- 2) **Content** – What is it people need to know?
- 3) **Purpose** – Why is it people need to have this kind of knowledge?
- 4) **Time** – When will this occur, or when will it be completed?
- 5) **Location** – Where is this happening?

¹ Stephen Lieb, Principles of Adult Learning, Senior Technical Writer and Planner, Arizona Department of Health Services, South Mountain Community College, VISION, Fall 1991.

Remember to listen for the information that will help you understand the kind of question being asked, and that will help you respond in the best way you can. If you can't answer a question, make a note of the speaker and their contact information. Encourage people to note questions on their evaluation forms. Some questions can be answered later through memos and notes on the office Intranet.

Some facilitators find it helpful to use questions as a way to manage or direct the conversation. Some types of questions are more helpful than others. For example, an open question that doesn't require a "right" answer or a question that is open to the whole group to answer can get conversation started: *What do you think of this kind of training as a way to educate staff?* On the other hand, a question that asks for a very specific answer (closed) or is directed to one individual may cause anxiety and shut down the conversation before it starts.

If you encounter a lot of resistance, you may need to call for a break. Most times you can deal with resistance by acknowledging it, deflecting or redirecting it, and moving on. Often a reminder "we are here to discuss..." is sufficient. If there is a persistent attempt to hijack the agenda, consider spending ten minutes to discuss the issue but no more. Remember there are others who came to your session because they were interested in the topic you are there to talk about.

2.2 Other suggestions

You may find it useful to remember the following tips for running the session:

- Participants are there to learn through active involvement; for example, through large and small group discussion, through reflection, through brainstorming.
- Be aware of who hasn't asked a question or offered a comment. Build in opportunities to give everyone a chance to contribute.
- If your equipment breaks down, don't worry. You have your presentation notes; participants have their handouts.

2.3 Facilities, equipment and supplies

Some presenters like to create their own tool kits including extra masking tape, markers, paper, pencils/pens, extra copies of handouts etc. Remember to:

- Confirm your room bookings.
- Find out if there are any special requirements for participants. These include scent free guidelines, allergies, and accessibility issues.
- Review your list of supplies and equipment needs before each session. You will need a computer with CD availability and a projector to show the presentation slides. You may also need to use a microphone depending on the ambient noise in the workshop room.
- Make sure you have enough chairs.
- Create a friendly environment: welcome people as they come in, have refreshments available at the start, or adjust the lighting in the room.
- Have a clock to help you keep to time, or ask a colleague to signal you.

2.4 Before you begin

Arrive at least 30 minutes before the scheduled start to:

- set up and check equipment
- distribute handouts
- check the lighting and curtains
- lay out nametags and markers
- organize your materials in the order you plan to use them
- find out necessary exits and washrooms as required
- set up your flipcharts

It is always helpful to have the title of the session on your screen so people can confirm they are in the right session.

SECTION III: AGENDA FOR FACILITATORS

FULL DAY SESSION Agenda		
Time	Activity	Components
6 hours	Full day	9 am to 12 noon one hour lunch, 1 pm to 4 pm
9:00a 30 minutes	A: Introduction	Review agenda Identify learning expectations Participant introductions
9:30a 15 minutes	B: Assessment	Identify what participants know or don't know about privacy List any concerns about privacy legislation
9:45a 1 hour	C: Legislation Overview Part One	Custodian's role Obtaining consent Collecting and using personal health information
10:45a 15 minutes	Break	
10:45a 1 hour	C: Legislation Overview Part Two	Disclosure of personal information Access & correction of personal health information Security of personal health information
11:45a 15 minutes	D: Discussion & Conclusion	Review key concepts Summarize
12:00p 1 hour	Lunch Break	
1:00p 1 hour	E: Scenarios	Small group discussion 45 minutes Large group discussion 15 minutes
2:30p 30 minutes	F: PHIA Tool Kit Resource Review	Legislation Policy Framework On-line Training Information Material (Articles)
2:30p 15 minutes	Break	
2:45p 1 hour	G: Creating & supporting a culture of Privacy	Developing & Implementing Policy for your Organization Addressing Concerns
3:45p 15 minutes	H: Conclusion	Review key concepts Complete evaluation form

SECTION IV. EDUCATION SESSION

A: SESSION OVERVIEW & INTRODUCTIONS (30 MINUTES)

In this section we have provided the key points for your introduction:

- A) Review the material in advance.
- B) Some people like to transfer the information we have listed in this section (Overview & Introductions) to index cards rather than reading straight from the sheet.
- C) Each of the slides (except the first one) begins on a new page. This format also applies to each subsequent component of the day.

TITLE SLIDE ON SCREEN

A. Opening the session

Begin on time. Introduce yourself to participants and welcome them to the session. Thank them for their interest and their commitment to the people they work with and for in the health system.

B. General comments

Everyone in Newfoundland and Labrador who works in the health and community services sector is subject to the *Personal Health Information Act*. The aim of the Act is to keep personal health information confidential and secure, while allowing for the effective delivery of health and community services. This education session will help everyone who works with personal health information to understand his or her responsibilities under the Act. Your organization will have policies to help you comply with the Act. Please refer to these policies for detailed guidance.

Review the overall agenda and explain the main parts:

- 1) process issues
- 2) education session structure

Process issues -- Explain any relevant housekeeping issues such as

- 1) turning off cell phones or setting them to vibrate
- 2) the location of washrooms
- 3) the anticipated break(s) and end of the session

Education session structure -- Present the session agenda. This session is in five parts:

- a) the presentation of the act,
- b) group discussion (scenarios)
- c) resources for implementation
- d) creating & supporting a culture of privacy through effective policies and practices
- e) concluding review of questions and perspectives

End this overview of the session by drawing attention to the participant's workbook containing the following:

- a) presentation handout
- b) scenarios
- c) the copy of the Act
- d) summary articles
- e) glossary
- f) evaluation form

C. Introductions

If you have a small group (up to 15 people), you can take a few minutes to ask people to identify themselves and share their reasons for attending today's session. If you have a mixed group, you may find it helpful to first ask the various groups to identify themselves by raising their hands. This will also help identify the wealth of collective knowledge in the group. If your group is larger than 15 participants, you can ask them to just state their name and occupation.

B: ASSESSMENT

SLIDE: ASSESSMENT (15 MINUTES)

To reinforce the message that everyone present is here to learn, take 10 to 15 minutes to identify what participants know or don't know about privacy. First ask participants to turn to their worksheet in their workbook called Assessment. Ask them to take a couple of minutes to jot down the answers. It is okay if they don't know the answers to the questions.

Go through each question quickly and ask participants to share the answers to the group as a whole. Make a short list on the flip chart. You can also probe the group by asking them for examples of privacy breaches or to recall any failures to protect personal information. You can also ask participants to name any concerns about privacy legislation. Use the notes on the flipchart to organize your conclusion at the end of the session and to consider what else participants may need to know or do to meet their responsibilities under the Act.

Some sample questions:

- *Do you need a patient or client's consent to use their personal health information in a research study?*
- *Your patient or client is unconscious. How much can you tell his relatives about condition?*
- *Can you send test results to doctors?*
- *Is it okay to use a patient's records to prepare their bill?*
- *As a custodian, what are your responsibilities under the Act?*

C: PERSONAL HEALTH INFORMATION ACT OVERVIEW PART ONE (1 hour plus 15 minute break)

NOTE: Technically this is slide 3 in the deck, but it is the first slide in the formal presentation. It is also numbered 1, and each slide then follows in sequence.

SLIDE 1. AGENDA

This presentation is an overview. It is important to take the time to read the act and to understand its provisions. It gives the participants information on the key components and principles embedded in the Act.

1. Overview
2. Custodian's responsibilities
3. Obtaining consent
4. Collecting and using personal health information
5. Disclosing personal health information
6. Requests for access and correction of personal health information
7. Security of personal health information
8. Other aspects of the Act
9. Conclusion

SLIDE 2: A NEW APPROACH

2.1 Overview

The Newfoundland and Labrador *Personal Health Information Act* (often abbreviated as PHIA) is a provincial law that governs the collection, use and disclosure of personal health information. The Act applies to all organizations and individuals involved in providing health and community services, administration and research in the public, private, health, and education sectors.

The Act balances an individual's right to privacy with the day-to-day practical requirements of providing health and community services. Everyone who works with personal health information must protect, collect, use and disclose that information in accordance with the Act.

2.2 History of the Act

In 2006, the Provincial Government approved in principle the *Health Information Act*, a draft Bill at the time. During the fall of 2006 and spring 2007, government officials organized public and stakeholder consultations to collect feedback and input into the proposed legislation.

In July 2007, the Provincial Government approved the Bill, known as the *Personal Health Information Act*, for introduction into the House of Assembly. The House of Assembly passed the *Personal Health Information Act* (PHIA) in June 2008, and the act became law in Newfoundland and Labrador. Proclamation of PHIA is expected for December 2010.

2.3 PHIA is a new way of thinking

The Personal Health Information Act is intended to foster a new way of looking at privacy. While all organizations will have a privacy officer, one person *alone* cannot do the job. All employees should understand the importance of keeping certain information confidential. PHIA applies to *everyone* who works with personal health information.

SLIDE 3: CULTURE OF PRIVACY

PHIA supports the development of a *culture of privacy*. **This means an organization is aware of and manages effectively and responsibly its obligations under PHIA part of its commitment to serving its clients.**

When an organization has a culture of privacy, the following happens:

- *Staff members communicate key privacy and security messages;*
- *Staff members avail of education on privacy issues across the organization;*
- *Staff members understand and respect the importance of reporting privacy-related incidents;*
- *The organization builds privacy into the fabric of the organization's activities (also known as privacy by design); and*
- *The organization makes privacy information and guidance readily accessible.*

SLIDE 4: WHY?

4.1 Purpose of the Act

PHIA creates *consistent rules* for the protection of personal health information in both public and private settings. The Act supports *transparency and accountability* practices. PHIA *clarifies and codifies* the appropriate *balance* between two important principles:

- (1) protecting individuals' privacy and
- (2) using individuals' personal health information for legitimate health-related purposes.

Legitimate health related purposes include

- *Health care,*
- *Planning and monitoring of the health system,*
- *Health research (oversight by research ethics boards or committees), and*
- *Public safety.*

4.2 Exclusions

There are some exclusions allowed under PHIA:

- the ***Child, Youth and Family Services Act*** establishes specific rules for the collection, use and disclosure of personal information.
- the rules governing information collected under the ***Adoption Act*** are, by necessity, significantly different from those governing information to which PHIA applies.
- the ***Youth Criminal Justice Act*** is a federal statute and information collected, used or disclosed in ensuing programs is subject to federal law.

SLIDE 5: WHAT?

5.1 What is contained within the Act?

PHIA establishes a comprehensive set of rules for the collection, use and disclosure of *personal health information*. Personal health information is defined broadly in the Act.

Personal health information includes information that can be used to identify an individual. This information could include their name, address, MCP, social insurance number or other contact details. Personal health information also includes information relating to the physical or mental health of an individual, as well as the care provided to them. Examples include: test results, family health history, treatment records, registration information, details of medication, referrals, payments for treatment etc.

Personal health information may be oral or recorded, so it could be the subject of a conversation or phone call or it could be a hand written, printed or electronic record.

From the Act: (...) "personal health information" means identifying information in oral or recorded form about an individual that relates to

- a. the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family;*
- b. the provision of health care to the individual, including information respecting the person providing the health care;*
- c. the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;*
- d. registration information;*
- e. payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care;*
- f. an individual's entitlement to benefits under or participation in a health care program or service;*
- g. information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service;*
- h. a drug as defined in the Pharmacy Act , a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or*
- i. the identity of a person referred to in section 7.*

SLIDE 6: ROLES

6.1 Who is responsible within the Act?

PHIA applies to custodians involved in the delivery of health care services in both the **public and the private sectors** in Newfoundland and Labrador. Under the Personal Health Information Act, a custodian is an individual or organization that has custody or control of personal health information. A full list of custodians is provided in the Act. Custodians of personal health information include:

- health professionals in private practice
- ambulance services
- Regional Health Authorities
- the Department of Health and Community Services
- Workplace Health and Safety Compensation Commission
- Four faculties at Memorial University
- the Newfoundland and Labrador Centre for Health Information

The way an organization is run may determine whether or not it is a custodian. For example, a long-term care facility run by a Regional Health Authority is not a custodian but the Regional Health Authority is a custodian. A personal care home that is run privately is a custodian. Individuals may be custodians. For instance, a physiotherapist who owns her practice is a custodian. However, the employees, contractors, volunteers and students of custodians are not custodians. For example, a physiotherapist who works for a Regional Health Authority is not a custodian.

Under PHIA, custodians must, among other things:

- Designate a contact person (s. 18, PHIA)
- Ensure confidentiality agreements for all employees, agents, contractors and volunteers are in place (s. 14, PHIA)
- Establish agreements with “information managers” (s. 22, PHIA)
- Establish detailed privacy and security policies and procedures (s. 13, s. 15, PHIA)
- Provide a privacy and security training program (s. 14, PHIA)
- Ensure a written statement of information practices is available to the public (s. 19, PHIA)
- Ensure the public is aware of notices of purposes for which personal health information is collected, used and disclosed through posting or directly providing to clients (this ensures that consent is knowledgeable (s. 20, PHIA)
- Maintain records or logs of disclosures (s. 48, PHIA)
- Maintain a process for managing limited consent /lock box requests (s. 37, PHIA)
- Implement a privacy breach management protocol (s. 14, PHIA)

Slide 7: RESPONSIBILITIES

Obligations under PHIA depend on your role. Before you can determine your obligations under PHIA, you need to know what your **role** is under the Act.

- Are you a *Custodian*? *Information manager*? *An employee of a custodian*?

The glossary provides a description of each of these roles.

As an employee of a custodian, your responsibilities include:

- (1) Respecting the organization's oath of confidentiality
- (2) Understanding how the organization's information policies are implemented
- (3) Supporting the creation of a culture of privacy in the organization
- (4) Participating in education about privacy and protection of personal information

When you take the oath or affirmation, you agree that the personal health information you come into contact with in the course of your employment, contract or service will remain confidential. Depending on organizational policies, the oath or affirmation may require you to agree that the personal health information shall remain confidential forever. If you haven't already taken an oath or affirmation, check with your supervisor who will make sure this is arranged.

PHIA provides the principles that must be respected to ensure the protection of personal health information. Depending on the services provided by the organization or individual, how this information is protected may differ from organization to organization. All custodians must develop and provide policies which guide the collection, use, storage, and disposal of personal health information. Use these policies to guide your work.

In a little bit, we'll discuss the ways you can support a culture of privacy in your organization. Remember: whatever your role, it's up to you to be familiar with the Act and to comply with its provisions. You must not access or use personal health information except as needed to do your job.

SLIDE 8: OBTAINING CONSENT

8.1. Obtaining Consent Under PHIA

The Act has been written to address several issues around consent that are specific to the health and community services sector. In many situations, the Personal Health Information Act requires you to obtain an individual's consent to collect, use or disclose their personal health information. It is important to understand that obtaining consent to collect, use and disclose personal health information under the Personal Health Information Act is different from obtaining an individual's consent to receive treatment.

These two types of consent must be considered separately and this course only considers consent to collect, use and disclose personal health information. Consent under the Personal Health Information Act may be either implied or express. In addition, there are certain uses and disclosures for which the individual's consent is not required (*i.e.*, for authorized health research, where approval from ethics boards or committees is obtained).

8.2 Implied consent

Implied consent is a form of consent that may be reasonably inferred from signs, actions, or facts, or by inaction or silence of an individual. Implied consent exists between healthcare providers treating a patient (*i.e.*, the "circle of care"). When an individual seeks health and community services, it is reasonable to assume that you have their implied consent to collect, use and disclose their personal health information, but only for the purpose of providing that health care service.

8.3 Express consent

Express consent is a form of consent that is obtained when an individual actively indicates (either verbally or in writing) that they agree to their personal health information being collected, used or disclosed for a specific purpose. There are situations where you need to obtain an individual's explicit permission to collect, use and disclose their personal health information for specific purposes. This permission is known as **express consent**. Express consent may be verbal or written. Express consent is required before:

- personal health information is disclosed to someone who is not a custodian and is not included in the circle of care (e.g. an individual asks their doctor to send medical information to their insurance company)
- personal health information is disclosed to another custodian for purposes other than providing health and community services.

8.4 Limited consent under PHIA

Where consent is required, an individual may place a condition or restriction on their consent to collect, use or disclose their personal health information. This situation is known as limited consent and the instruction given by the individual is known as a consent directive. Examples of limitations include:

-
- an individual limiting access to their profile in an Electronic Health Record
 - an individual requesting that a family member who works for the custodian must not see their record.

Limited consent does not prevent a custodian from collecting personal health information where this is required by law or by normal professional or institutional practice. Limited consent provisions do not apply to collections, uses and disclosures of personal health information that are permitted without consent (e.g., disclosures for research purposes; MCP billing; etc.). Some organizations require all requests for limited consent to be directed to the contact person.

When an individual limits their consent for the collection, use or disclosure of personal health information, it is important that they are informed of any potential negative impacts on their care. PHIA requires that the consent directive be recorded in such a way that it is available to anyone who may use or disclose the personal health information.

SLIDE 9: COLLECTION & USE

9.1 Collecting personal information

PHIA identifies all circumstances under which the collection, use and disclosure of personal health information is permitted, **both with and without consent**. There are general rules governing how personal health information is collected and used. There are exceptions to the general rules; for example, another Act may require the particular collection of data. PHIA makes it clear which **collections** require an individual's consent, and which do not.

The collection of personal health information means to gather, acquire, receive or obtain the information by any means from any source. Examples include interviewing an individual, referring to notes or viewing information on a computer screen.

In general, you must not collect personal health information unless you have the individual's consent (implied or express). ***You must only collect personal health information that is reasonably necessary to meet the purpose of the collection.***

Collection may be direct or indirect. Direct collection of personal health information means to collect that information directly from the individual or from an authorized individual acting on their behalf.

Examples of direct collection include:

- a pharmacist gathering information from an individual during a consultation
- a doctor in an emergency gathering information from a parent of a child following an accident.
- a social worker performing a family assessment

Where you gather the information directly, you are required to inform the individual or the representative providing the information on their behalf, why it is being collected, and of the expected uses and disclosures.

Indirect collection of personal health information means to collect the information about an individual from someone other than the individual themselves. Some examples of indirect collection that you will encounter are:

- where an individual has asked someone to provide personal health information (e.g. an individual asks a dentist to forward an x-ray to another dentist)
- where a custodian receives information from another custodian (e.g. a laboratory receives information about an individual from a doctor).

Where you gather the information indirectly, it is not your responsibility to inform the individual why it is being collected.

9.2 Using personal health information

The general rule is that custodians may only use personal health information for the purpose for which it was collected. However, personal health information may also be used in other

situations specified under the Act. PHIA makes it clear which uses of personal health information are permitted; for example:

- Planning, delivery of health care services / programs;
- To obtain payment for services; public health or safety; and
- For the purpose of risk management or error management.

Using personal health information means handling or dealing with it:

- by a custodian and the people who have taken an oath or affirmation of confidentiality required by the custodian
- for the purpose for which the information was collected.

You may only use an individual's personal health information:

- when the use is lawful and consent has been obtained

OR

- when the use without consent is required or permitted by the Act.

The use of personal health information must be limited to those who need to know the information to carry out their duties. Use does not include disclosure. The Act allows the personal health information of an individual to be used without their consent for certain purposes. You should always remove the names and other identifiers from the information before you use it. We call this process de-identification. For example, if you were reviewing a list of visits to a clinic to determine which day of the week was busiest, you could remove names and other identifiers from the other information.

Break time

C: PERSONAL HEALTH INFORMATION ACT OVERVIEW PART TWO (1 hour)

SLIDE 10: DISCLOSURE

10.1 Disclosing Personal Health Information

In the Personal Health Information Act, disclosure means to make the information available or to release it, but does not include the **use** of the information. For example, when a family doctor refers an individual to a specialist and sends details of the individual's symptoms, the doctor is disclosing personal health information to the specialist.

You may not disclose personal health information unless:

- you have the individual's consent or
- the disclosure is permitted or required by the Act without the individual's consent.

When you are disclosing information, you should only disclose the minimum information required for the purpose for which the receiving party will use it. You should not disclose personal health information if other information will serve the same purpose.

There are some exceptions to this rule. If an individual is unable to give consent, their personal health information may be disclosed to another health professional or custodian so that the individual can receive safe and timely health care. Custodians may contact a relative in emergency, where a court order requires, or where this disclosure is required by another act. Again, PHIA makes it clear which **disclosures** require an individual's consent, and which do not.

There are certain situations in which personal health information must be disclosed ***even if you don't have the consent of the individual***. These include:

- *Registry of personal health information*
- *Electronic Health Record*
- *Investigations and legal proceedings*

A registry is a population-specific listing of people who have a condition that has significance to the overall health of a particular population. Some registries have been given special authority to collect information without the consent of the individual. You will receive information about these registries before you disclose personal health information to them. The registries are listed in the regulations under the Personal Health Information Act.

The Newfoundland and Labrador Centre for Health Information operates an information network across the province to support safe and timely care and services. No consent is required to disclose personal health information to designated parts of the information network (e.g. the Pharmacy Network).

You must disclose personal health information for the purposes of aiding certain investigations or legal proceedings. In larger organizations, the health records department might deal with such disclosures.

The Act considers disclosures outside of the province separately from disclosures within the province. Though many of rules are similar, it is important to consult the Act when considering disclosures outside of the province. If you encounter a situation where disclosure outside the province is required, check your organization's procedures. If in doubt, talk to your contact person for guidance.

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

SLIDE 11: ACCESS & CORRECTION

11.1 Requests For Access And Correction Of Personal Health Information

The Personal Health Information Act provides individuals with the right to access their personal health record and the right to request correction of that record (subject to specific exceptions). Some examples where a custodian may deny requests for access include:

- *if there is a risk of harm to the individual or another person as a result of gaining access to the record; where a legal investigation is underway; or*
- *if the request is frivolous or vexatious in any way.*

PHIA identifies the process and timelines for accessing personal health information files and requesting corrections or annotations. The Act identifies the responsibilities of custodians respecting access to and correction of records containing personal health information.

Custodians may require access requests to be in writing and organizational policies may require all such requests to be forwarded to your designated contact person. In larger organizations the contact person will often transfer the request to a department such as Health Records. It is important to understand your organization's policies associated with individuals who request access to their own information.

The Act does not prevent a custodian from granting an individual access to their personal health information where the individual makes an oral request for access (or even when the individual makes no request). These informal requests may arise where an individual asks to see or correct their personal health information directly during a conversation with their healthcare provider.

Unless your organization's policies indicate otherwise, you may show an individual their records in response to an informal request.

Many custodians, including all Regional Health Authorities, have existing policies that prohibit employees, agents, volunteers, and students from directly accessing their own health records.

If your organization does not allow you to directly access your own records, you must not do so. It may be a disciplinary offence. If you want to see your own health records, you must follow the normal procedures and make an application to the custodian or contact person.

SLIDE 12: PROTECTION

12.1 Information policies and procedures

PHIA requires that custodians establish policies and procedures to protect the personal health information in their custody or control. Custodians must have policies and procedures to:

- Protect confidentiality of information in their custody
- Restrict access on a need-to-know basis
- Protect information stored, used or disclosed outside the jurisdiction
- Provide for the secure storage, retention and disposal of information

Personal health information may be maintained in both electronic and paper format. It is important that custodians protect the personal health information in their custody or control, regardless of its format.

The Act does not prescribe specific security controls. Each custodian must assess and manage the risk inherent in its own operations. Custodians must implement information security safeguards and controls to protect the personal health information in their custody or control. Your organization will have developed security procedures that are appropriate for its mandate. It is your responsibility to be familiar with these procedures and to follow them.

12.2 Security measures

Information security is the process by which the confidentiality, integrity, and availability of information are safeguarded and ensured.

No one product, process, policy or technology alone can protect personal health information. Effective information security requires the successful integration of:

- **Physical** security controls, such as door locks, alarm systems and private working areas;
- **Administrative** security controls, such as policies, procedures and guidelines documents; and,
- **Technological** security controls, such as firewalls, antivirus and encryption.

Controls of all three types must be developed to work together to create an effective information security framework.

You can help to protect personal health information in your workplace by following some straightforward guidelines.

- Store documents containing personal health information in a secure container such as a locked filing cabinet when left unattended.
- Where possible, clear your desk and lock away personal health information at the end of the workday.
- Avoid accidental exposure of personal health information (shoulder surfing).
- If there are restricted areas in your workplace, look out for anyone who is not authorized to be there.

12.3 Disposal

Personal health information must be disposed of in a secure manner. Here are some guidelines:

- Paper records of personal health information should be shredded and not simply thrown in the garbage.
- CDs and other media should be physically destroyed.
- Personal health information held on a computer or in the memory found in other electronic equipment, such as photocopiers and scanners, should be magnetically erased or overwritten in such a way that the information cannot be recovered. These types of destruction will generally be handled by an IT professional.

Your organization must have procedures for the secure dispose of personal health information securely. If you are the custodian, you must ensure you have a process for secure disposal. If you are the employee, you must ensure you follow the procedures.

SLIDE 13: PRIVACY BREACHES

13.1 Breaching The Act

Unauthorized collection, use, or disclosure of personal health information is a breach of the Personal Health Information Act. These situations include losing or stealing personal health information or disposing of it in an ineffective or inappropriate manner.

If you believe that a breach has taken place, or that personal health information is at risk, here is what you must do. If you are an employee of a custodian, you must report it to your supervisor, manager or contact person. These people need to know about the breach in order to control it, investigate it, and implement any remedial action.

If you are the custodian, you may need to take further action. For example, custodians must notify individuals if their personal health information is breached, except when the custodian believes there will be no adverse impact to the individual. Custodians must notify the Privacy Commissioner in the event of a material breach.

Even though the breach may be unintentional, it is important that all breaches are reported.

13.2 Consequences

The Act specifies the consequences for breaching the act. People who violate the terms of the act may be fined \$10,000, may face six (6) months in prison where a person willfully (i.e., intentionally) contravenes a provision of PHIA, or both. There are also similar penalties for custodians or information managers who fail to protect personal health information as they are required to under the Act.

Custodians may be subject to penalties even if they violate the Act without intent.

As an employee of a custodian, you may be subject to disciplinary action by your employer including termination of your employment. You may also be subject to disciplinary action by the regulatory authority that governs your profession.

Deliberate disregard includes:

- attempting to obtain personal health information by false pretences
- destroying personal health information to evade a request for access to the information
- knowingly using personal health information for unauthorized purposes (for example using addresses to update a Christmas card list or accessing a family member's test results out of curiosity)
- misleading or obstructing the Information and Privacy Commissioner or another person exercising powers under the Act.

SLIDE 14: OTHER PROVISIONS

14.1 Review by Privacy Commissioner

The Act also identifies the powers, responsibilities and accountabilities of the Office of the Information and Privacy Commissioner (OIPC) in the context of the Act. The OIPC can investigate any alleged breach of the Act, inform the public about the Act and make recommendations to ensure compliance. An individual may make an appeal directly to the Supreme Court, Trial Division or following a review by the OIPC.

14.2 Legislative Review

At least every five years, the Act will undergo a formal review. The Minister responsible for the legislation will appoint a special committee to carry out the review. The committee will submit its report to the Minister, with any recommendations for change as required.

14.3 Good Faith

The “Good Faith” clause provides custodians and their employees with immunity from civil liability (*i.e.*, private lawsuits) while appropriately performing their duties. **Good faith** means a sincere and reasonably-held belief that an action was proper and lawful, or a motive to act in a proper and lawful way, without malice or an intent to defraud. It has a specific, legal meaning with respect to the Act.

14.4 Compliance Essentials

The Act offers specific requirements by custodian to ensure compliance. These include:

- Designating a contact person (s. 18)
- Ensuring confidentiality agreements for all employees, agents, contractors and volunteers are in place (s. 14)
- Establishing agreements with “information managers” (s. 22)
- Establishing detailed privacy and security policies and procedures (s. 13, s. 15)
- Providing a privacy and security training program (s. 14)
- Ensuring a written statement of information practices is available to the public (s. 19)
- Ensuring the public is aware of notices of purposes for which personal health information is collected, used and disclosed through posting or directly providing to clients (this ensures that consent is knowledgeable (s. 20)
- Maintaining records or logs of disclosures (s. 48)
- Maintaining a process for managing limited consent /lock box requests (s. 37)
- Implementing a privacy breach management protocol (s. 14)

D: FACILITATED DISCUSSION (15 MINUTES)

Slide 15: DISCUSSION

In this part of the session, you will guide participants through a discussion of what they have learned, any questions they may have, and any suggestions they would like to share.

Ask these questions to stimulate discussion:

- *What are your expectations with the new changes?*
- *Where do you think will be the greatest effects from this new legislation?*
- *If you have questions or concerns, how might you address them?*

If the conversation gets stuck, remind people gently that every issue can't be solved in the discussion. You can also direct the question to other participants by asking:

- Does anyone have any suggestions on how to deal with this issue?

At the end of the discussion, summarize the key points raised by participants. If there are unanswered questions, make sure they have been written down on a flip chart. You may contact the Office of the Privacy Commissioner or the Newfoundland and Labrador Centre for Health Information for more detailed responses to questions arising in the sessions.

SLIDE 16: CONCLUSION

It is important to remember these four keystones:

- ***Legislation lays the foundation*** and mandates policy development
- ***Organizations develop policy*** to guide employees practice
- ***Custodians combine privacy principles with best practice***
- ***Employees support culture of privacy*** and protection of PHI

NOTE: At this point in the session you will take a one hour lunch break. It is important to remind everyone that they should plan to return at least 10 minutes before the session starts so that they may get ready for the second part of the education session.

LUNCH BREAK

E: SMALL GROUP DISCUSSION (SCENARIOS) (60 minutes)

Welcome everyone back after the lunch break. Remind them to turn off their cell phones to avoid causing disruption in the class. Take a few moments to gauge the atmosphere in the room. Ask people if they are comfortable and ready to begin. This next part will focus on group discussion and learning together.

SLIDE 17: SCENARIOS

The scenarios (without the answers) are included in the participants' workbook. Split the group into two or three smaller groups. Each group has 30 minutes to review the scenarios, discuss any issues, and identify the answers. After the 30 minutes, bring everyone back together.

Ask:

- *How did you feel about that exercise?*
- *What made you think?*
- *What did you learn?*

Now go through the answers quickly.

Ask:

- *Was there anything that surprised you?*
- *How comfortable did you feel about dealing with the issues raised in the scenarios?*
- *Any other thoughts?*

When we talk about scenarios, it allows us to make certain ideas more concrete. Sharing experiences where staff can discuss questions that arise helps promote greater understanding. It also sends a message that other staff can help, staff can use policy and procedures to guide responses, and that looking for more information is always a good approach.

1) A physician working at a hospital requires a series of blood tests for one of his patients. This situation will mean that the patient's personal health information will be made available to the nurse who cares for the patient and the laboratory technician who carries out the tests.

Question: Which one of the following statements is correct?

- A The nurse may assume implied consent but the laboratory technician will require express consent.
- B Both the nurse and the laboratory technician may assume implied consent.
- C Both the nurse and the laboratory technician will require express consent.

Answer: B: The doctor, the nurse and the laboratory technician are all providing care to the patient and so are within the circle of care. While they remain within the circle of care, they may all assume the implied consent of the patient.

2) Jenny Brown has been admitted to hospital for surgery. Her ex-husband works in the radiology department. Jenny doesn't want him to see any of her health records.

Question: Can she limit her consent so that her ex-husband does not see her personal health information?

Answer: Yes, she may use a consent directive to limit the collection, use and disclosure of her personal information. This directive could state that her ex-husband should not be able to see her records. Staff at the hospital should inform her about the possible consequences of this directive.

3) Sarah Chapman is a senior physiotherapist. She has been asked to provide an opinion on whether her group should invest in additional ultrasound machines. Sarah wants to gather evidence based on the use of the single machine they currently own. To gather this evidence she will have to use the records of all patients treated using ultrasound for the past year.

Question: Which one of the following statements is correct?

A Sarah may use the records for this purpose.

B Sarah may only do this if she has the express consent of all the patients involved.

Answer: This would constitute evaluation of a health care program or service, so it is a permitted use under the Act without consent. Sarah may carry out her assessment without obtaining the express consent of the patients involved. If reasonable, she should remove the names of the patients before working with the information. Also, she must not include names or other identifying information in any reports she produces.

4) Kathy Simmonds is the office manager for a group of dentists. One of the dentists has just completed treatment of a patient who had a broken tooth. Kathy now needs to use the patient's record to generate an itemized bill.

Question: Which one of the following statements is correct?

A Kathy may use the records for this purpose.

B Kathy may only do this if she has the express consent of the patient.

Answer: A: The Act allows the use of personal health information for the purpose of obtaining payment for the provision of health care or related goods or services. Kathy may use the patient's record without obtaining their consent.

5) An individual at a community clinic fell while walking into the building. Sheila Brennan, a manager, has been asked to complete an occurrence report as part of quality and risk management processes aimed at improving safety. Sheila will need to use information

about the care and treatment the individual received in relation to the fall to complete her report.

Question: Which one of the following statements is correct?

- A Sheila may use the records for this purpose.
- B Sheila may only do this if she has the express consent of the individual involved.

Answer: A: The Act allows personal health information to be used without consent for risk management purposes. Sheila may use the information without obtaining the consent of the individual involved.

6) William Grant is suffering from lower back pain. He asks Dr Evans, his family doctor, to send copies of his X-rays and a note about his condition to his chiropractor.

Question: Is Dr Evans disclosing William's personal health information by sending the note and X-rays?

Answer: Yes: Dr Evans will be disclosing William's personal health information when she sends the note and X-rays to the chiropractor. Dr Evans is responding to William's request, so she has his express consent to disclose the information.

7A) Adam Green has been in a road accident involving a moose. He is unconscious and has been picked up by the ambulance service and taken to the emergency department of the nearest hospital. The paramedic on the ambulance has done an assessment of his vital signs.

Question: May the paramedic disclose the assessment results to the Emergency Room team?

Answer: Yes: Disclosure is necessary for the provision of health care and is allowed without consent because consent cannot be provided in a timely manner (Adam is unconscious).

7B) Adam Green is now in intensive care. He has not regained consciousness. Sarah Jones is the nurse manager on the inpatient unit. Adam's brother arrives to visit him and asks Sarah "How is my brother Adam Green doing?"

Question: May Sarah disclose this information to Adam's brother?

Answer: Yes: Sarah may disclose limited information to someone she can reasonably believe is his immediate family, a relative or has a close personal relationship with Adam. When Adam regains consciousness, Sarah should let him know that she has talked to his brother and obtain Adam's consent for any future disclosure.

If you are in doubt about how to respond in situations like this, refer to your organization's policies on providing updates on individuals under your care.

8) Janice Green is the manager at a large residential care home. She is archiving her residents' records and is packaging them up to be sent to an information manager specializing in storage of personal health information.

Question: May Janice send the records to the information manager for storage without the consent of individual residents?

Answer: Yes: By sending the records to the information manager for storage, she is disclosing personal health information. However, disclosing personal health information to an information manager is allowed without consent.

9) Stephen Harrison is recovering from a stroke. He is discussing his treatment with an occupational therapist, Linda Fletcher. Linda is making notes on Stephen's progress. Stephen asks if he can read the notes.

Question: Which one of the following statements is correct?

- A Stephen does not have the right to see his notes.
- B Linda must refer Stephen to the contact person.
- C If her organization's policies allow, Linda may show Stephen the notes she has made.

Answer: C: The Act provides Stephen with the right to access his personal health record. Linda's notes are part of his record. Many organization's policies require access requests to be in writing. However, if her organization's policies allow, Linda may show Stephen the notes she has made. Even if Linda cannot show Stephen the notes at this time, Stephen can still make a formal request to see them.

10) Dr Maitland is a physician working for a Regional Health Authority. He wants to check the accuracy of his own personal health information and his position means that he has access to all health records including his own.

Question: Does PHIA give Dr Maitland the right to directly access his own records?

Answer: No: All Regional Health Authorities have existing policies that prohibit individuals from directly accessing their own health records. Dr Maitland is prohibited from directly accessing his own records and PHIA does not give him the right to do so. If Dr Maitland wishes to see his health records, he must follow the organizational procedures of the Regional Health Authority.

11) Neil Burton is a dental hygienist in a private dental practice. As he is walking through reception, he notices that patient records are clearly visible on the receptionist's computer screen. He is concerned that people who have come into the office may have seen them.

Question: What should Neil do?

- A He doesn't need to take any action.
- B Ask the receptionist to be more careful with her screen but not mention it to anyone else.
- C Ask the receptionist to be more careful with her screen and tell the head of practice (who is also the custodian). (correct)

Answer: C: It's possible that personal health information has been inadvertently disclosed. Neil must report this possible breach to the custodian. Neil should also ask the receptionist to turn the screen around or use another monitor until the issue is addressed.

F: PHIA RESOURCES (30 minutes)

The purpose of this component is to start participants on the path of integrating what they have learned in the morning (theory and principles) with their current and future practice (policy development, education, and support).

Slide 18: PHIA Resources (30 minutes)

In partnership with several provincial stakeholders, the Department of Health and Community Services has created several resources to assist custodians of personal health information to meet their obligations under the Act. Custodians are not obligated to use these resources. Custodians should review the materials carefully and make appropriate use them to facilitate their compliance with the *Personal Health Information Act*.

Legislation

The Act is available on-line (most current version) and in paper form from the Queen's Printer. There is a copy in the Participants' Workbook. The Act is available on the Government of Newfoundland and Labrador's website at:

<http://www.assembly.nl.ca/legislation/sr/statutes/p07-01.htm>

The PHIA Risk Management Toolkit

A comprehensive guide to information security and risk management is available on the Department of Health and Community Services' website.

The *Personal Health Information Act* requires that custodians protect the personal health information in their custody or control. The Act requires that custodians take steps that are reasonable in the circumstances to ensure that personal health information in their custody or control is:

1. protected against theft, loss and unauthorized access, use or disclosure;
2. protected against unauthorized copying or modification; and,
3. retained, transferred and disposed of in a secure manner.

To meet these obligations custodians should incorporate risk management processes into their projects, activities and systems as early as possible; ideally, during the design or planning phases. Risk management can be defined as being the identification, assessment, and prioritization of risks followed by a coordinated and efficient application of resources to minimize, monitor, and control the likelihood and impact of adverse events.

The PHIA Risk Management Toolkit is intended to:

-
- Assist custodians of personal health information and other stakeholders in understanding their legislative- and policy-based obligations as they relate to the safeguarding of personal health information;
 - Assist custodians in assessing their current state of compliance with PHIA;
 - Assist custodians in assessing the effectiveness of the physical, administrative and technological controls that they have established to protect the personal health information in their custody or control; and,
 - Assist custodians in identifying any gaps or areas for improvement that there might be in their physical, administrative and technological controls.

The PHIA Risk Management Toolkit contains the following items:

1. Information Security Management Overview
2. Privacy Checklist
3. Preliminary Privacy Impact Assessment
4. Privacy Impact Assessment
5. Privacy Audit
6. Privacy Breach Guidelines
7. Privacy Breach Reporting Form

PHIA Policy Development Manual

A comprehensive guide to developing policy is available on the Department of Health and Community Services' website.

The *Personal Health Information Act* requires that custodians have policies and procedures in place that describe the ways that they collect, use and disclose personal health information. The PHIA Policy Development manual is intended to provide custodians with a framework for developing their own policies and procedures to meet this obligation.

The PHIA Policy Development Manual sets out the legal requirements of the *Personal Health Information Act* and arranges those requirements into a policy framework. The manual provides custodians with sample policy and procedure language: the sample policy language reflects custodians' obligations under the *Personal Health Information Act* while the sample procedure language contains suggestions as to how the policies could be implemented.

Custodians should not simply adopt the sample policies and procedures in this policy development manual as their own; rather, custodians should review the samples provided and customize them in order to make them applicable to their particular activities and line of business. It should always be kept in mind that, while custodians may customize the sample language provided in the PHIA Policy Development Manual, custodians should be careful to ensure that whatever policies or procedures they develop are legally compliant with the requirements of the Act. Custodians should consult the Act, their regulatory authority and/or

solicitor for interpretation of or for guidance on the provisions of the *Personal Health Information Act*, where necessary and as applicable.

PHIA Online Education Program

The Department of Health and Community Services has developed an on-line training tool for self-learning and assessment on PHIA. The training modules have two components: one for custodians and one for non-custodians. Because the program is password based, on-line learners can complete the course at their own pace by logging in for different sessions. For example, the participant could focus only on the sections dealing with consent one day or complete the section on security another. The on-line modules are designed to take about 45 minutes for non-custodians and one hour for custodians. Much of the material for this session has come from the on-line training module to ensure consistency.

Ask:

What else might you need to help you meet your obligations under PHIA?

NOTE: When you ask this question, you are helping people to problem solve. Other people may have useful suggestions they can share. If you are the custodian, the answers you hear in the session may help you link staff with more appropriate information and resources.

Break

G: IMPLEMENTING PHIA IN YOUR ORGANIZATION (1 HOUR)

SLIDE 19: Implementing PHIA (1 hour, approximately 20 minutes on the first two components and 10 minutes on the third component and the summary)

Having spent a little time learning about what resources you have available to you, we are now going to spend some time on three issues:

- Creating & supporting a culture of privacy
- Developing & implementing policy for your organization
- Addressing concerns

In this way, you can start to think practically how you will incorporate the principles you have learned to meet your obligations under the Act (depending on your role as a Custodian, information manager, employee).

With each component, record comments and ideas from participants on the flip chart. This will help them focus on generating practical suggestions for immediate and short-term implementation.

SLIDE 20: Privacy Culture

This morning we talked about how PHIA supports the development of a *culture of privacy*. When an organization has a culture of privacy, the following happens:

- *Staff members communicate key privacy and security messages;*
- *Staff members avail of education on privacy issues across the organization;*
- *Staff members understand and respect the importance of reporting privacy-related incidents;*
- *The organization builds privacy into the fabric of the organization's activities (also known as privacy by design); and*
- *The organization makes privacy information and guidance readily accessible.*

Questions for Group Discussion

- *How will you create a culture of privacy in your organization?*
- *What messages are you promoting about privacy?*
- *What training can you offer to staff (link to on-line training modules)?*
- *What processes do you have/need for reporting privacy related issues?*
- *What steps can you take to build privacy by design into your organization?*
- *How accessible are your policies and practices on protecting health information (patient/client advisory)?*
- *What are you doing now?*
- *What else do you need to do to meet the obligations of PHIA?*

Don't forget to record comments and ideas on the flipchart.

SLIDE 21: Developing Policy

This morning we talked about policies and procedures that manage the collection, storage, sharing, and disposal of personal health information. Let's go back to the policy framework document included in your workshop package.

- *How will you develop new policies supporting privacy and protection of health information in your organization?*
- *What policies do you have in place now?*
- *What areas are missing?*
- *What else do you need to meet the obligation of PHIA?*

Don't forget to record comments and ideas on the flipchart.

SLIDE 22: ADDRESSING CONCERNS

When we started this morning, some of you identified some concerns about PHIA. (Refer to the flip chart notes from the Assessment).

- *Have you any other concerns?*
- *Have your questions been answered?*
- *How will you hear about concerns from staff?*
- *How will you help staff deal with questions?*
- *How might you resolve them?*
- *What else do you need to meet the obligations of the Act?*

Don't forget to record comments and ideas on the flipchart.

Looking at the three areas we discussed, we can see that there are a lot of good ideas on moving forward in creating and supporting privacy and protection of personal health information. Some themes we can see include

NOTE: *Take a moment to identify emerging themes. You can group them very simply. The idea is to reinforce the message about protection of personal health information as a way of working, not as a one-time only activity.*

H: CLOSING AND EVALUATION (15 MINUTES)

SLIDE 23: CONCLUSION

PHIA does not represent a radical departure from existing privacy legislation. If you are compliant with ATIPPA and/or PIPEDA, your organization is well on the way to being compliant with PHIA.

There are many resources that have been developed, and which are intended to be used as templates. These include policies, agreements, risk management tools, etc. This session is one example of the ways staff members in health organizations are learning about PHIA.

Two important points as you get started on creating and supporting a culture of privacy in your organization:

- 1) Get started as early as possible.
- 2) Understand your roles and obligations and make any adjustments to current policies / procedures that might be necessary.

This is the concluding part of the session, where you summarize the key points of the presentation (what you want participants to “take away” with them).

The new Act embodies a focus on protecting personal health information and creating a culture of privacy

Implementing the provisions of the new Act will be an evolving process as everyone works together to ensure understanding and clarity.

There are resources available to provide guidance and to inform best practices.

Your observations of how this process unfolds are important. The Act will be reviewed every five years. It is important to recognize what is working well and what needs to be improved.

Ask participants: what is the most important thing you learned at this session?

SLIDE 24: REFLECTION

Another way to ask participants to reflect on what they have learned is by focusing on:

- Head: What is the most important thing you learned today?
- Heart: How do you feel about what you learned here?
- Hands: What will you share with your coworkers about your experience here today?
- Feet: What have you learned that you can put into practice right away?

Evaluation is an important part of this process. Your comments on the education session today will be helpful to those whose sessions are coming later. Please take a few minutes to fill out the evaluation form so that we can make any necessary changes to the presentation structure for remaining sessions.

Thank you for your attention and we look forward to continuing this conversation on how we can create a culture of privacy in our organization.

SLIDE 25: CONTACT INFORMATION

This slide contains contact information for PHIA. You may also customize it to provide the contact information for your specific organization (i.e. health authority, university faculty, medical centre etc.).

For more information custodians should consult with their regulatory bodies (e.g., the Newfoundland and Labrador College of Physicians and Surgeons, the Association of Registered Nurses of Newfoundland and Labrador, etc.) and / or with their legal counsel for further information.