



Personal Health Information Privacy and Access Act

Nancy Lindsay
Chief Privacy Officer
May 12, 2011

Presentation Plan



- ↳ New Legislations
- ↳ Compliance with Personal Health Information Privacy and Access Act

New Legislation

Right to Information and Protection of Privacy Act (100 sections) RTIPPA

Ø Replaces: Right to Information Act (1978)
(16 sections)



Personal Health Information Privacy and Access Act (81 sections) PHIPAA

Ø Replaces: Protection of Personal Information Act (1998) (10 sections)



Personal Health Information Privacy and Access Act

Personal Health Information Privacy and Access Act (PHIPAA)

- ↳ Applies to all organizations or individuals that collect, maintain, use or disclose PHI for the purpose of:
 - § Providing health care or treatment
 - § Planning and managing the health care system
 - § Delivering a government program or service
- ↳ These are referred to as custodians

Examples

- Public bodies
- Health care providers
- the Minister
- AmbulanceNB
- NB Health Council
- **RHAs**
- Researchers
- A lab or specimen collection centre
- Workplace Health, Safety and Compensation Commission
- The Canadian Blood Services
- Information managers
- Health care facilities
- Nursing homes

Personal Health Information (PHI)

Means identifying information about an individual relating to:

- § the individual's physical and mental health
- § family history or health care history, including genetic information about the individual
- § registration information, including the Medicare number
- § the provision of health care



Personal Health Information (cont'd)

- § Payments or eligibility for health care or health care coverage
- § Donation of body part or bodily substance including his or her genetic information
- § Identifying the individual's substitute decision maker
- § Identifying his or her health care provider

Definition of Record

Means a record of information in any form, and includes

- information that is written, photographed, recorded, or stored in any manner, on any storage medium or by any means, including by graphic, electronic or mechanical means, but does not include electronic software or any mechanisms that produce records.

Purposes of the Act

- ü Right to examine and receive a copy of PHI
- ü Right to correct and amend PHI
- ü Provides rules regarding the collection, use, disclosure, retention and secure destruction of PHI
- ü Facilitates effective provision of care and planning and management of the health care system

Purposes of the Act

- ü Provides mechanisms to ensure the accountability of custodians
- ü Provides independent review and resolution of complaints
- ü Provides mechanisms to safeguard PHI security and integrity
- ü Provides effective remedies for contraventions of the Act

Impacts of other Legislations

- § The *Medical Consent of Minors Act* remains applicable with this Act
- § The *Mental Health Act* prevails over this Act
- § *PHIPAA* prevails over other Acts unless they provide more protection



Privacy Principles

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use,
Disclosure and
Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging
Compliance

Principle 1: Accountability



Accountability

- The Chief Privacy Officer has been appointed to ensure compliance with the Privacy Legislation
- Every employee and non-staff personnel has the responsibility to ensure that the personal health information which we maintain and control is protected from unauthorized collection, use or disclosure.
- Every employee or non-staff personnel has the responsibility to report a potential or actual breach.

Principle 2: Identifying Purpose



Purpose for collection, use and disclosure of PHI

The custodian is obligated to provide an explanation for the collection, use and disclosure of PHI

This may be done through the posting of a notice which describes the purpose where it is likely to come to the individual's attention or by providing a copy to the individual

Principle 3: Consent



Consent must be knowledgeable

Consent is knowledgeable if the individual knows:

- The purpose for the collection, use or disclosure
- He/she may withhold or withdraw their consent at any time
- That it relates to their PHI
- That it may not be obtained through deception or coercion
- That it may be implied or express

Types of Consent

Implied Consent:

- If we have posted a notice to explain the purpose for the collection, use and disclosure of PHI, and the individual provides the information, then we can assume the individual has provided implied consent to collect, use or disclose their PHI for that purpose.

Types of Consent

Continuing Implied Consent:

- If we have received personal health information from an individual relating to that individual, for the purpose of providing health care to that individual, the custodian is entitled to assume that we have their continuing implied consent to collect, use or disclose the PHI for that purpose of providing health care.

Types of Consent

Express Consent:

- Individual must consent in writing
- Usually we are releasing the PHI to a third party not providing health care to the individual such as:
 - The media
 - For fund raising activities
 - A third party such as a lawyer or insurance company
 - Researcher

Types of Consent

Conditional Consent:

- This Act provides the individual with the right to direct who may use, disclose and retain his/her personal health information

Exceptions:

- If prohibited by law
- Related to a program to monitor certain classes of drugs
- Related to the creation and maintenance of an electronic health record

Principle 4: Limiting Collection



Collection of PHI

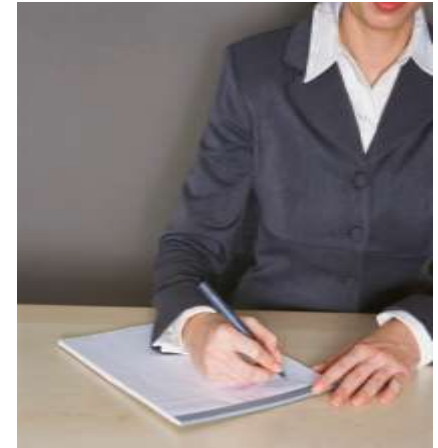
General duties of custodians

§ Collection of PHI

- Ø Obtain consent
- Ø Explain the need for collection

§ Collection of PHI without consent when

- Ø Consent cannot be obtained
- Ø Necessary for the provision of health care



Scope of Collection of PHI

The Custodian may not collect

- ∅ more PHI than to fulfil the purpose of the collection
- ∅ PHI if other information is available

De-identified information

The Custodian may collect PHI for any purpose

Notice of collection practices

Custodian who collects PHI informs the individual of

- ∅ Purpose of the collection
- ∅ How to contact an officer or an employee (if the custodian is not a health care provider)



Source of Information



PHI collected directly from the individual **except** if:

- Ø Individual has authorized another method of collection
- Ø Collection would endanger the individual's health or safety
- Ø Collection of the PHI is in the individual's interest
- Ø Inaccurate PHI might be collected
- Ø Research project approved by a research review body is being carried out
- Ø Authorized by Court order, Act of the Legislature or Parliament of Canada, treaty
- Ø Substitute decision maker can act on the individual's behalf
- Ø PHI is collected for the purpose of assembling a family history

Principle 5: Limiting Use, Disclosure and Retention



Use of Personal Health Information

General duty of custodians

- § Use of PHI must be limited to
 - Ø Minimum amount of information necessary
 - Ø Staff and employees who need to know it

De-identified information

- § Custodian may use it for any purpose



Disclosure of Personal Health Information

A Custodian may disclose PHI only to:

- Ø The individual or to his or her substitute decision maker
- Ø Someone else if consent has been obtained

Disclosure of Personal Health Information without consent

Disclosure without Consent

1. for health related purposes
2. for health care programs or other programs
3. for health and safety purposes
4. for proceedings
5. for enforcement purposes
6. for research purposes

Requirements for retention, storage and secure destruction

A custodian establishes and complies with a written policy

- ü Meets requirements prescribed by regulation
- ü Protects privacy
- ü Keeps a record of:
 - Individual whose PHI is destroyed
 - Summary of contents
 - Related time period
 - Method of destruction
 - Supervisor's name

Principle 6: Accuracy



Accuracy of Information

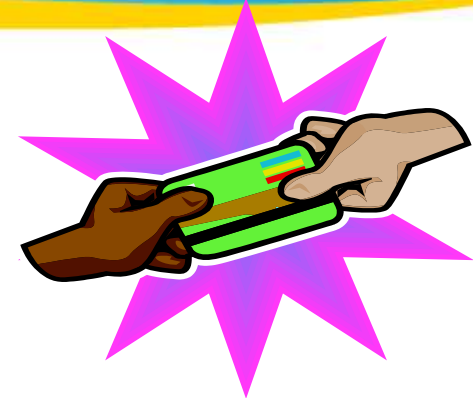
Custodian ensures the information is:

Ø Accurate

Ø Up-to-date

Ø Complete

Ø Disclosed to the authorized person



Medicare Number

Collection of a Medicare number can only be:

- Ø For the provision of health care
- Ø To verify the individual's eligibility to a health care program
- Ø For the payment and to manage the health care system

We must inform the individual that we have a legal authority to ask for his or her Medicare number

Principle 7: Safeguards



Safeguards

- Administrative, technical, physical safeguards to ensure confidentiality, accuracy and integrity of the information
- § Information technology security standards taking into account the level of sensitivity of PHI

Administrative Safeguards

Policies and Procedures

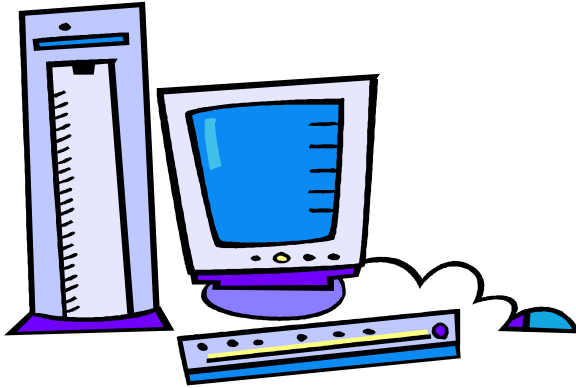
- Corporate Privacy Policy
- Privacy Breach Policy
- Confidentiality Policy
- Privacy Impact Assessment

Draft:

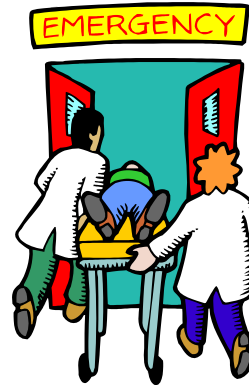
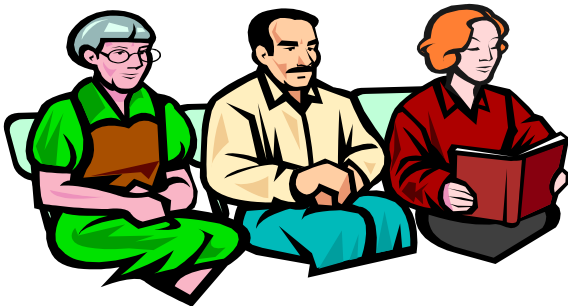
- Confidential Information Sharing Policy



Technical Safeguards



Physical Safeguards



Physical Safeguards



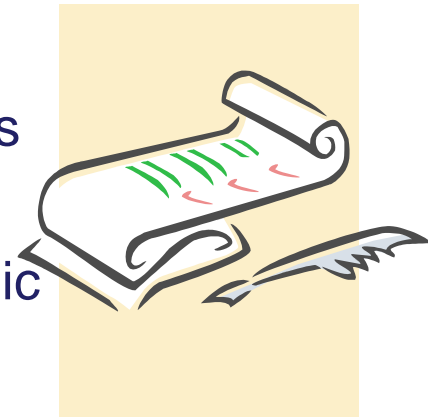
Principle 8: Openness



Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal health information.

- Public privacy statement
- Publish person responsible to receive complaints
- Publish a toll free number
- Obligation to make policies and procedures public



Principle 9: Individual Access



Right to examine and to copy PHI

- Right to view and to have a copy of their PHI
- Request:
 - Ø Made to the custodian
 - Ø Detailed
 - Ø In writing



Right to examine and to copy PHI

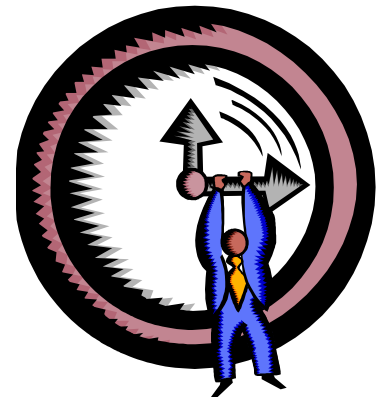
(continued)

The custodian has a duty to assist an individual when we receive a request without sufficient details



Custodian's Response

- § Free examination
- § A 30-day time limit to respond
- § Extension of the 30-day time limit is possible upon request To Privacy Commissioner
- § The transfer of a request must be made within 10 days following the request's arrival
- § The reproduction fees are defined as per the regulations of the Act



Right to Request a Correction of PHI

The custodian has an obligation to have PHI that is accurate and complete.

An individual will make

§ Written request for a correction

The custodian within 30 days of receiving a request will

§ Correct the PHI or

§ Inform the individual in writing that

- The PHI no longer exists
- The PHI is maintained by another custodian and, if possible, provide that custodian's contact information.
- If correction refused will inform the individual of the reason and the individual's right to contest the decision

Principle 10: Challenging Compliance



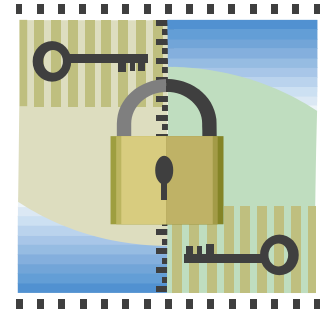
Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Chief Privacy Officer

The custodian must designate a person to:

- Ø Develop policies and procedures related to receiving complaints
- Ø Respond to inquiries from the public
- Ø Provide assistance and direction regarding privacy questions
- Ø Receive complaints from the public
- Ø Notify the individual and the Privacy Commissioner in the event of:
 - Theft or loss
 - Disposal
 - Disclosure to or access by an unauthorized person



Access to Information and Privacy Commissioner

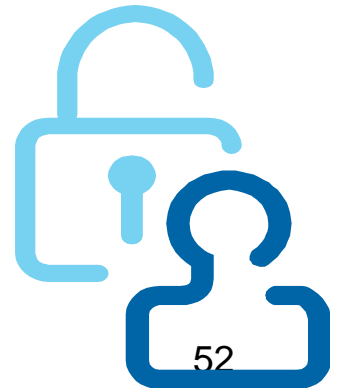
The Commissioner has the right to

∅ Enter any office of a custodian

- Examine or make copies of any record

∅ Converse in private with

- Any officer of the custodian
- Any employee of the custodian



Review

- Referral to the Commissioner
- Referral to a Judge of The Court of Queen's Bench



Offenses

A person who violates or fails to comply with the provisions of this Act commits an offence under Part II of the *Provincial Offences Procedure Act* as a category F offence.

Not an Offense

A person who provides a record/PHI/evidence to the Commissioner does not commit an offence under any other Act of the Legislature.





Bob Gray 2008

"THAT WILL BE \$28.75...NOW IF I CAN JUST GET YOUR POSTAL CODE, PHONE NUMBER AND A SMALL BLOOD SAMPLE.."

Thank you for your attention

Questions?