

The Health Information Protection Act

“HIPA 101”

....the basics of

The Health Information Protection Act

Saskatchewan Health

August 2005

Overview of Session

- ◆ New privacy world – federal and provincial legislation
- ◆ Brief history of development
- ◆ Overview of *The Health Information Protection Act*
- ◆ Getting Started....things to focus on

Privacy world is changing!!

◆ Provincial Legislation

- ◆ *The Health Information Protection Act*
- ◆ Applies to the health sector in Saskatchewan
- ◆ In development since 1997. In force September 1 2003.

◆ Federal Legislation

- ◆ *Personal Information Protection and Electronic Documents Act*
- ◆ Applies to “organizations” engaged in “commercial” activities
- ◆ In force for most as of January 1, 2004

PIPEDA

- ◆ Federal legislation – industry focused
- ◆ Provinces have worked to clarify application to health sector
- ◆ National health organizations have worked with federal government to develop interpretive guidelines
- ◆ Consent focused – may be implied

PIPEDA: Industry Canada suggests minimal impact

“Health professionals will have to ensure that they:

- ◆ ***Let patients know about the collection, use or disclosure of their personal health information.***
- ◆ ***Obtain consent to disclose information to third parties when appropriate.***
- ◆ ***Provide an individual with access to his or her own personal information.***
- ◆ ***Provide secure storage of information and implement measures to limit access to patient records.***
- ◆ ***Ensure proper destruction of information that is no longer necessary.***
- ◆ ***Inform patients of the organization's information-handling practices through various means (i.e. the posting of notices, brochures and pamphlets, and/or through normal discussions between a patient and a health care provider).”***

Source: Industry Canada website - PIPEDA Awareness Raising Tools (PARTs) Initiative For The Health Sector, March 2004

PIPEDA – help available!

- ◆ Industry Canada

 - ◆ www.strategis.ic.gc.ca/privacy/health

- ◆ Health Canada

 - ◆ www.hc-sc.gc.ca/ohih-bsi/theme/priv/privinfo_e.html

- ◆ Privacy Commissioner of Canada

 - ◆ www.privcom.gc.ca

- ◆ National and provincial professional bodies

HIPA is different!!

- ◆ Created for the health sector in Saskatchewan
- ◆ Does not require consent to be collected for core functions of trustees
- ◆ Rules for use and disclosure specific to the health sector

Why New Legislation?

- ◆ Old legislative structure very program specific:
 - ◆ *The Freedom of Information and Protection of Privacy Acts* only apply to government and local authorities.
 - ◆ Numerous health-specific statutes.
- ◆ Increasing demand for sharing information/system development with integration of health services.
- ◆ Saskatchewan Health Information Network (SHIN).
- ◆ Growing concern over privacy.

History of Development

- ◆ Consultation on key issues in Fall of 1997.
- ◆ Consultation on draft legislation in Winter of 1997-98; Fall of 1998, February 1999.
- ◆ Passed by the Legislature in Spring 1999.
- ◆ Information sessions and consultation on regulations Fall and Winter 2000-01.
- ◆ Consultations on amendments Fall and Winter 2001-02
- ◆ Amendments Spring 2003
- ◆ Proclamation September 1, 2003
- ◆ Consultation on regulations Summer and Fall 2004
- ◆ First set of regulations came into force July 2005

Overview – what we will cover...

- ◆ Key definitions – (trustee, personal health information)
- ◆ Scope of the Act
- ◆ Rights of the Individual
- ◆ Duties of Trustee to Protect Personal Health Information
- ◆ Rules for Collection, Use and Disclosure
- ◆ Access to records, the Commissioner, penalties

Who must comply?

- ◆ The Act applies to:
 - ◆ trustees,
 - ◆ with personal health information.
 - ◆ There are exceptions.

A trustee includes.....(*subsection 2(t)*)

... the following (with custody and control):

- ◆ government institutions
- ◆ regional health authorities and affiliates
- ◆ special care homes
- ◆ personal care homes
- ◆ mental health facilities
- ◆ laboratories
- ◆ pharmacies
- ◆ community clinics
- ◆ Saskatchewan Cancer Agency
- ◆ ambulance operators
- ◆ regulated health professions
- ◆ health profession regulatory bodies
- ◆ others can be added through regulations

Personal Health Information

- ◆ The Act applies to “personal health information”: (*clause 2(m)*)
 - ◆ information about the health of an individual;
 - ◆ information with respect to a health service provided to an individual;
 - ◆ information collected incidental to providing health service;
 - ◆ registration information.

Exceptions

- ◆ The Act does not apply to: *(section 3)*
 - ◆ statistical or de-identified information
 - ◆ administrative information or other records of a trustee

- ◆ HIPA prevails over all other statutes in regard to personal health information – with limited exceptions: *(section 4)*
 - ◆ *The Public Health Act 1994, The Mental Health Services Act, The Workers Compensation Act, Part VIII of The Automobile Accident Insurance Act, Section 16 of The Cancer Foundation Act, The Vital Statistics Act, The Adoption Act, The Child and Family Services Act, The Public Disclosure Act*

Rights of the Individual

(sections 5 to 15)

- ◆ Right to consent (expressed or deemed) to most use and disclosure *(section 5)*
- ◆ Right to revoke consent *(section 7)*
- ◆ Right to be informed *(section 9)*
- ◆ Right to know to whom information is disclosed outside the circle of care *(section 10)*
- ◆ Right to access records held by a trustee *(section 12)*
- ◆ Right to review by commissioner *(section 14)*

Safeguards – Duty to Protect *(section 16)*

- ◆ A trustee must have administrative, technical and physical policies and procedures that:
 - ◆ Protect the integrity, accuracy, confidentiality, and security of the information
 - ◆ Protect against loss, or unauthorized access to or use, disclosure or modification of the information
 - ◆ Ensure compliance with this Act by its employees

Safeguards – Retention and Destruction *(section 17)*

- ◆ A trustee must:
 - ◆ *Retain* records for the period specified in regulations *(not yet proclaimed)*
 - ◆ Ensure that records are *stored* in a way that they are readable, retrievable and useable
 - ◆ *Dispose* of records in a safe manner that protects the privacy of the individual (e.g. properly shredded, if paper)

Information Management Service Providers

(section 18)

- ◆ Processes, stores, archives, combines or destroys personal health information for trustee
- ◆ Provides information management or technical services
- ◆ Written agreement required between trustee and IMSP (*this subsection is not yet proclaimed*)
 - ◆ Governs access to and use, disclosure, storage, archiving, modification & destruction of information
 - ◆ Provides for protection of information
 - ◆ Meets requirement in regulations
- ◆ IMSP must comply with agreement
- ◆ Trustee as an IMSP

Duty to Protect – others

(section 19 to 22)

- ◆ Duty to ensure accuracy
 - ◆ Reasonable steps, when collecting
- ◆ Duty where one trustee discloses to another
- ◆ Duty disclosing to persons other than trustee
- ◆ Continuing duty of trustees
 - ◆ A trustee cannot simply abandon records
 - ◆ Must care for them or transfer to another

Collection, Use and Disclosure: General Rules *(section23)*

- ◆ Collection, use and disclosure on a need-to-know basis
- ◆ Policy and procedure must limit access by employees who do not require the information
- ◆ De-identified information should be used where practical

A trustee may collect personal health information *(section 24) ...*

- ◆ For a program or service that will benefit the individual
- ◆ If it is consistent with a use or disclosure authorized by the Act
- ◆ If permitted by law
- ◆ With consent

Collection should be *(section 25)*...

- ◆ Direct from the individual except:
 - ◆ The individual consents to collection from elsewhere
 - ◆ Individual cannot provide the information
 - ◆ Collection from the individual would cause harm
 - ◆ Collection is to determine eligibility of the information to participate in a program of the trustee
 - ◆ Information is available to the public
 - ◆ Information is collected for a use or disclosure authorized by the Act
 - ◆ Prescribed circumstances
 - ◆ Family medical history

A trustee may use personal health information *(section 26)*...

- ◆ With consent, or:
 - ◆ For a purpose consistent with a disclosure authorized by the Act (i.e. if it is OK to disclose, it is OK to use)
 - ◆ To de-identify the information
 - ◆ For a purpose that will primarily benefit the individual
 - ◆ In accordance with regulations
- ◆ Cannot be used for employment purposes, except with consent
- ◆ Must have policy and procedure limiting access to a need to know

Disclosing Personal Health Information *(sections 27 to 29)*

- ◆ Any purpose with expressed consent
- ◆ With deemed consent for “circle of care”
- ◆ For limited purposes without consent
- ◆ If registration information, as provided for in section 28
- ◆ For research, if it meets the tests in section 29

Disclosure – Deemed Consent

(subsection 27(2)) “the circle of care”

- ◆ Consent is deemed to exist:
 - ◆ “for the purpose of arranging, assessing the need for, providing, continuing, or supporting the provision of, a service requested or required by the subject individual” *(subsections 26(2) and 27(2))*
- ◆ Trustee must have policy and procedure limiting disclosure to those who need to know
- ◆ Health professionals must satisfy the ethical practices of the profession *(subsections 23(2) and 27(3))*

Disclosure without Consent: examples

(subsection 27(4))

- ◆ To prevent or minimize danger
- ◆ To contact next of kin for compassionate circumstances
- ◆ To obtain payment for services
- ◆ To administer an estate
- ◆ For peer review, standard of care review
- ◆ To legal counsel, for court order
- ◆ For program delivery, evaluation, monitoring, planning (limited disclosure, must retain confidentiality)

Disclosure of Registration Information

(section 28)

Information collected to register a person for a service

- ◆ By Sask. Health to a trustee for provisions of services
- ◆ By Sask. Health to another government institution, regional health authority or Sask. Cancer Agency to verify accuracy/eligibility
- ◆ Between Sask. Health and regional health authorities, affiliates and Sask. Cancer Agency for program delivery, evaluation, monitoring, research, planning
- ◆ Of limited information to school boards
- ◆ By ministerial agreement

Use and Disclosure for Research

(section 29)

- ◆ Does not apply to de-identified information
- ◆ With consent:
 - ◆ approval of research ethics committee
 - ◆ researcher must agree to keep confidential, provide appropriate security, return or destroy as required by agreement
- ◆ Without consent:
 - ◆ all of the above, and
 - ◆ must not be reasonably practical to obtain consent and research cannot be done with de-identified
 - ◆ Research ethics committee must believe benefits outweigh risk to privacy

Access by Individuals to Their Own Personal Health Information *(sections 31 to 40)*

- ◆ Trustee must provide access to individual's own information
- ◆ Request to access can be oral or written
- ◆ Trustee must respond to written request within 30 days
- ◆ Trustee may charge reasonable fee to recover costs
- ◆ Trustee may refuse access in limited circumstances
- ◆ Individuals have right to request amendments to information about themselves
- ◆ Individual may apply for review & appeal of trustee's decision

Information and Privacy Commissioner

- ◆ Independent Third Party
- ◆ Powers to investigate, review decisions, and make recommendations including:
 - ◆ Review access decisions
 - ◆ Review alleged contraventions
 - ◆ Comment on proposed legislation or programs of trustees
 - ◆ Carry out investigations re: personal health information in custody or control of trustee to ensure compliance with HIPA
 - ◆ Conduct public education programs

Penalties for violations *(section 64)*

◆ Individuals:

- ◆ Can be fined up to \$50,000 and/or receive up to one year in jail per offence

◆ Corporations:

- ◆ Can be fined up to \$500,000 per offence
- ◆ Officers and directors of a corporation can be fined up to \$50,000 and/or receive up to one year in jail per offence

◆ Good faith clause to protect trustees and employees

HIPA – Summary

- ◆ Applies to health sector and government
- ◆ Creates duty to protect personal health information
- ◆ Creates rules for collection, use and disclosure
- ◆ Supports the “circle of care”
 - ◆ Consistent with ethical practices of profession within the circle
 - ◆ Strict rules for use and disclosure outside the circle
- ◆ Provides right of access by individual
- ◆ Establishes third party oversight

Regulations

- ◆ Consultations over August and September 2004
- ◆ Examples:
 - ◆ Fees for accessing personal health information
 - ◆ Retention periods
 - ◆ Disclosure for certain fundraising activities
- ◆ First set of regulations came into force July 2005
- ◆ Review and development of other proposed regulations ongoing

Getting started.... keeping it simple!!

- ◆ Establish a privacy officer or person(s) responsible for privacy and security matters
- ◆ Conduct a review of current practices
- ◆ Do an inventory of personal health information
- ◆ Conduct a gap analysis
- ◆ Develop a plan to fill in gaps
- ◆ Implement and monitor

Getting started.... Key areas of focus

◆ 6 key areas:

1. Access
2. Security
3. Consent
4. Collection and Use
5. Disclosure
6. Policy and Procedures Required

Getting started.... Access

- ◆ Review current practice
- ◆ Is practice in compliance with HIPA?
- ◆ Key things to consider
 - ◆ Individual has right to access their information
 - ◆ Exceptions
 - ◆ Fee
 - ◆ Written response within 30 days
 - ◆ Individual can request review and appeal

Getting started.... Security

- ◆ Review current practices
- ◆ Look at sections 16 and 17 of HIPA for compliance
- ◆ Key things to consider
 - ◆ Secure files
 - ◆ Limit access to need-to-know
 - ◆ Safe destruction of records
 - ◆ Contracts that protect your interest

Getting started.... Consent

- ◆ Review current practices
- ◆ Is practice in compliance with HIPA?
- ◆ Key things to consider
 - ◆ Deemed consent - circle of care
 - ◆ Outside the circle of care – implied or expressed and must be
 - ◆ oral/written, informed, voluntary, not obtained through misrepresentation, fraud or coercion
 - ◆ Without consent – only in accordance with the law

Getting started.... Collection & Use

- ◆ Review current practices
- ◆ Is practice in compliance with HIPA?
- ◆ Key things to consider
 - ◆ Is it for purposes of the program, activity or service of trustee
 - ◆ Limit to need-to-know basis
 - ◆ Purpose that will primarily benefit individual
 - ◆ In accordance with an Act or regulation
 - ◆ Collect directly from individual where possible

Getting started.... Disclosure

- ◆ Review current practices
- ◆ Is practice in compliance with HIPA?
- ◆ Key things to consider
 - ◆ Identify the Circle of Care – know what is in and what is not
 - ◆ Consent is deemed to exist
 - ◆ List disclosures to non-trustees
 - ◆ Consent or in accordance with the Act

Getting Started...Policy & Procedure Required

- ◆ Section 9 – To inform individual of anticipated uses, disclosures, and rights under the Act
- ◆ Section 16 – Protecting records
- ◆ Section 17 – Retention and disposal
- ◆ Section 23 – Limiting use to a need to know basis
- ◆ Section 27 – Limiting disclosure to a need to know basis

Getting started.... summary

- ◆ Appoint a leader
- ◆ Consider the six key areas
- ◆ Know your circle of care
- ◆ Don't re-invent the wheel –
 - ◆ develop common standards, policies and practices within your own health profession

Information

- ◆ Saskatchewan Health: www.health.gov.sk.ca
- ◆ Saskatchewan Information and Privacy Commissioner: www.oipc.sk.ca
- ◆ PIPEDA: www.strategis.ic.gc.ca/privacy/health
- ◆ Privacy Commissioner of Canada: www.privcom.gc.ca