KO Telemedicine

# Privacy Considerations for First Nations Telemedicine


Presenters:

***Gregory Ward:*** Quality Assurance/Privacy Officer, KO Telemedicine

***Brendan Seaton***: Consultant, Trusted By Design

# Why Privacy?

- What does privacy mean to you?
- What does privacy mean to your community?

# Privacy is not about….

- Compliance with legislation
- Compliance with government requirements
- Interference by governments or privacy commissioners
- Bureaucracy
- Overburdening you with new tasks and responsibilities

# Privacy is about….

- You
- Your family
- Your community

- Its about:
  - Your rights as an individual
  - Your obligations as a health service provider

# Important Definitions

**Privacy** - The right of an individual to control the collection, use, disclosure and retention of their personal information

**Confidentiality** - The obligation of a health care provider (or other person) to protect the secrecy of personal information

**Security** - The tools and techniques we use to protect the confidentiality, integrity and availability of personal information.

# What is Health Information

- Individually identifiable health information
- Pseudonymized or anonymized information used for research purposes
- Aggregated information for management reporting purposes

# Issues of concern to First Nation's Communities

**Concerns for the "Individual":**

- The confidentiality of personal health information, especially in small communities
- The accuracy of information that is used to make decisions about healthcare and entitlements
- The use of information for secondary purposes not related to health care

# Issues of concern to First Nation's Communities

**Concerns for the "Community":**

- Protection against negative portrayals, stigmatization, misinterpretation, or misuse of data
- Confidentiality of traditional cultural practices
- Relevance to the questions, priorities and concerns of the community

# Individual and Collective Privacy

- Individual and collective privacy should be considered as complementary
- They represent two levels of protection for First Nations Peoples
- Concepts of individual privacy are well established in the broader Canadian population and are encoded in legislation
- Concepts of collective privacy are unique to, and recognize the rights of First Nations communities

# Fair Information Practices

- Fair Information Practices in First Nations Communities are based on:
  - The CSA Model Code for the Protection of Personal Information (CSA Privacy Code) for individual privacy
  - Ownership, Control, Access and Possession (OCAP) Principles for collective privacy
- Most privacy legislation since 1996 has been based on the CSA Code

# Privacy Principles

There is nothing new or difficult about privacy. Good privacy is:

- Good business practice
- Good information management practice
- Good clinical and health care management practice

Organizations that have good business, information management and clinical management practices in place are likely in compliance with these principles already

# The Importance of Principles

- Consistent application of privacy rights locally, nationally and internationally
- Defines with precision the privacy obligations of people handling personal information
- Provides a sound basis for a privacy protection program

# The CSA Code and OCAP

- The CSA Privacy Code relates to the rights of individuals to control the collection, use, disclosure and retention of personal information

- The OCAP Principles relate to the rights of First Nations Communities to control the collection, use, disclosure and retention of information about the community (e.g. research studies)

# CSA Privacy Code

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

# Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

# Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

# Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

# Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

# Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

# Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

# Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

# Openness

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

# Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

# 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.

# OCAP Principles

- **Ownership**
- **Control**
- **Access**
- **Possession**

# OCAP as Collective Privacy

**Collective Privacy:** a second level of protection, consistent with cultures that value both individual and collective self-determination.

# OCAP as Collective Privacy

- OCAP protects community/collective information as Privacy protects individual information.
- Privacy of traditional cultural practices is well recognized. OCAP protects all community information.
- Collective privacy protects against negative portrayals, stigmatization, misinterpretation or misuse of data.
- Can be implemented through policies requiring community consent for data collection, data access, data sharing or reporting of results.

# Ownership

- Relationship of First Nations community to its cultural knowledge / data / information
- Community / group owns information collectively as individuals own personal information
- Distinct from possession (stewardship)

# Control

- First Nations aspirations & rights to maintain, regain control in all areas of their lives (includes research data)
- Control can include all stages of a project
- Control can extend to resources, policy, review processes, formulation of conceptual frameworks, data management, etc.

# Access

- First Nations must have access to information, and data about themselves and their communities, wherever it is held.
- First Nations communities and organizations have the right to manage and make decisions regarding access to their collective information.

# Possession

- Possession (stewardship) is a mechanism to assert, and protect ownership.
- When First Nations data is in the possession of others (e.g. government, academia), there is a risk of breech or misuse, especially when trust is lacking between owner and possessor.

# Privacy Laws

- The Federal Government, all Provinces and Territories have laws in place dealing with privacy in the government sector.
- Six Provinces have health specific privacy legislation (British Columbia, Alberta, Saskatchewan, Manitoba and Ontario, and Newfoundland/Labrador)
- Three Provinces have legislation in place dealing with privacy in the private sector (BC, Alberta, Quebec)
- All other provinces default to PIPEDA for privacy in the private sector.
- Laws deal with personally identifiable information

# Access Laws

- The Federal Government, Provinces and Territories have Access to Information Laws in place
- Purpose is to ensure openness and transparency in government
- Concerns about access to and control of de-identified information about First Nations communities that is in the control and possession of government organizations

KO Telemedicine

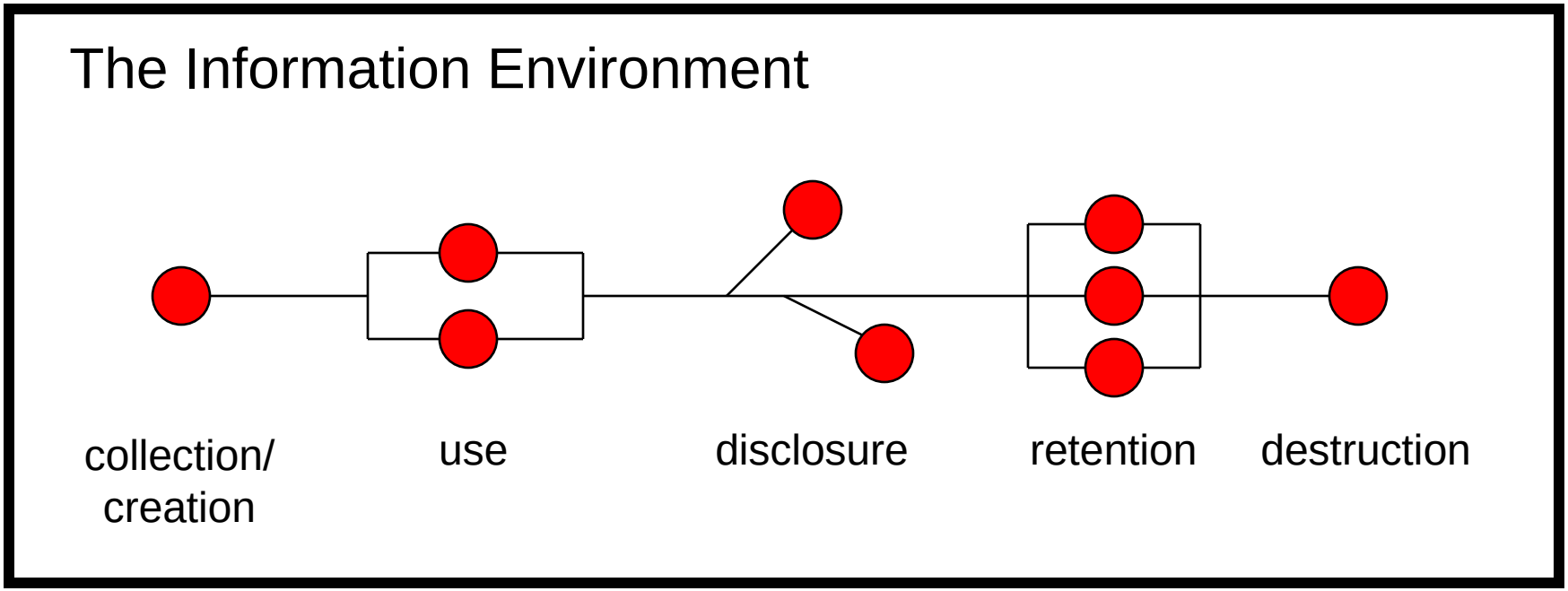
# KO Telemedicine:
# Privacy Impact Assessment (PIA)

# The Privacy Impact Assessment

- The PIA is a tool to:
  - help define **privacy requirements** for a new system or program
  - help identify **privacy risks** and to recommend actions to help manage those risks
  - inform management, regulators and patients about the **privacy features** of a system or program and to advise of any **residual privacy risks**.

# The PIA as a story…

The PIA describes the environment in which personal information lives, and tells the story of personal information from its collection or creation, through to its eventual destruction.



# The Story Should Have a Happy Ending

The PIA should describe privacy strengths as well as privacy weaknesses!

# Contacts:


- Gregory Ward
- (800) 387-3740 x 1311
- gregoryward@knet.ca

- Brendan Seaton
- (647) 880-6381
- brendan.seaton@ehealthrisk.com