Privacy and Security at CIHI
DPPS 2018 – Cal Marcoux

Canadian Institute for Health Information
CIHI: A trusted partner
CIHI’s Privacy and Security Program

• Maintains the trust and confidence of stakeholders

• Protects individual privacy, the confidentiality of records and the security of information
CIHI’s Privacy and Security Framework

Available at www.cihi.ca
Key Privacy & Security Program Components

- Privacy and security risk management
- Governance framework
- Policies, procedures and standards
- Secure Information Lifecycle
- Cybersecurity program
- Management Processes include;
  - Training and awareness, Audit & Assessment, Incident Management, Monitoring & Reporting, Continual Improvement
Privacy & Security risk management

- Risk Management is a formal, repeatable process to identify, assess, treat and monitor privacy and security risks

  Information Security Risk Management

  -> Privacy & Security Risk Management

  -> Corporate Risk Management

- Recognition that risk exists – it’s better to manage it than to be afraid of it

- Risk Management is embedded in everything we do
Privacy and Security Risk Management IN CONTEXT

Privacy and Security Framework

Information Security

- Enterprise Information Security Program Elements
- Information Security Management System

Privacy and Legal Services

- Enterprise Privacy Program Elements
- Legal Services Program Elements

Privacy and Security Risk Management
Governance Framework

- **Board committees** provide oversight to the privacy and security programs
- **Chief Privacy Officer & General Counsel** responsible for Privacy
- **Chief Information Security Officer** responsible for information security
Policies, procedures and standards

Examples

• *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data*

• *Information Security Policy*

• *Privacy and Security Incident Management Protocol*

• *Privacy Impact Assessment Policy*

• *Privacy and Security Risk Management Framework*

All available at [www.cihi.ca](http://www.cihi.ca)
Secure information lifecycle

- Creation and Acquisition
- Retention and Storage
- Access and Use
- Disclosure
- Disposition
Cybersecurity Program

Key cybersecurity components include;

- Perimeter monitoring and protection
- Endpoint monitoring and protection
- Antivirus, antimalware
- Authentication
- Encryption
Training and awareness: CIHI’s culture of privacy and security

CIHI’s staff are made aware of the importance of maintaining the confidentiality of personal health information and other sensitive information through mandatory privacy and security training and through ongoing communications about issues that may impact privacy and security at CIHI.
Audit and assessment - External review of CIHI’s Privacy and Security Program

- Prescribed entity under Ontario’s *Personal Health Information Protection Act* (PHIPA)
- CIHI maintains International Organization for Standards (ISO) 27001: 2013 certification
Audit and assessment – internal audit

- **Privacy audit program**
  - Program area audits
  - Topic audits
  - Data recipient audits
  - PIAs

- **Information Security audit program**
  - Vulnerability assessments, “ethical hacks”
  - Data access audits
  - Ad hoc audits
Incident Management

• Privacy and Security Incident Management Protocol allows CIHI to identify, manage and resolve privacy and information security incidents and breaches.

• An incident is any event that;
  – Affects or has the potential to affect the confidentiality, integrity or availability of CIHI’s information assets
  – Compromises or has the potential to compromise CIHI’s information security controls
  – May result in unauthorized use, access, copying, modification, disclosure or disposal of CIHI’s information assets.

• All staff are expected to report all actual, suspected or potential incidents
Monitoring & Reporting

• Ongoing monitoring of information security controls with monthly metrics and key performance indicators

• Monitoring of external environment
  – Threat/risk landscape
  – Relevant legislative and regulatory developments

• Management review of Information Security Management System and Privacy & Security Risk Management Program on an annual basis
Continual Improvement

• Privacy & Legal Services and Information Security collaborate daily and identify improvements through:
  – Program reviews
  – Incident management activities
  – Risk management activities
  – Proactive engagement of staff and governance bodies
If you could choose only 5 controls....

“Top 5” critical data protection controls:

1. Encryption of personal information
2. Patch management for all systems/software
3. Staff awareness – especially for phishing and other social engineering
4. Access management – respect the need-to-know principle
5. Data minimization – only collect, store, use data that is required for the purpose at hand
Questions?