

Privacy and Personal Health Information in Ontario

Fred Carter

Senior Policy/Technology Advisor

National Institutes of Health Informatics (NIHI)
App Developer's Guide to Privacy and Security

Tuesday January 31, 2016



Overview

Who We Are
PHIPA Overview
IPC Guidance
Questions / Exercises



Who We Are

- The Information and Privacy Commissioner (IPC) provides an independent review of government and health care decisions and practices concerning access and privacy.
- The Commissioner is appointed by and reports to the Legislative Assembly; and remains independent of the government of the day to ensure impartiality.

Mission and Mandate

- **MISSION:** We champion and uphold the public's right to know and right to privacy.
- **MANDATE:**
 - resolve access to information appeals and privacy complaints
 - review and approve information practices
 - conduct research
 - deliver education and guidance (on access and privacy issues)
 - comment on proposed legislation, programs and practices.

IPC and Technology

- Long history of engagement and advocacy
 - from PETS to PbD
 - Research and education
 - Complaints
 - Investigations
 - Comment on proposed projects
 - Involvement in external groups
 - Guidance

Ontario Access and Privacy Laws

- The *Freedom of Information and Protection of Privacy Act (FIPPA)*
 - applies to over 300 provincial institutions such as ministries, provincial agencies, boards and commissions, as well as community colleges and universities
- The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*
 - applies to over 1,200 municipal institutions such as municipalities, police services boards, school boards, conservation authorities and transit commissions
- The *Personal Health Information Protection Act (PHIPA)*
 - covers individuals and organizations in Ontario that are involved in the delivery of health care services, including hospitals, pharmacies, laboratories and health care providers such as doctors, dentists and nurses



Personal Health Information Protection Act (PHIPA)

- *PHIPA* came into force on November 1, 2004
- Majority of *PHIPA* governs “personal health information” in the custody or control of:
 - “Health information custodians” or
 - “Agents” of health information custodians
- However, the Act also has broader application
- For example, it contains restrictions on the use and disclosure of personal health information by non-custodians that receive personal health information from custodians



What is Personal Health Information?

- Personal health information (PHI) is identifying information about an individual relating to their health and health care, such as:
 - Clinical information
 - Family history
 - Health provider
 - Health number

Why is the Protection of Privacy So Critical?

- The need to protect the privacy of individuals' PHI has never been greater:
 - Extreme sensitivity of PHI
 - Greater number of individuals involved in the delivery of health care to an individual
 - Increased portability of PHI
 - Emphasis on information technology and electronic exchanges of PHI

Consequences of Inadequate Attention to Privacy

- Discrimination, stigmatization and psychological or economic harm
- Individuals avoiding testing or treatment
- Individuals withholding or falsifying information
- Loss of trust or confidence in the health care system
- Cost and time in dealing with privacy breaches
- Legal liabilities and proceedings

Sanctions for Unauthorized Access

- Investigation by privacy oversight bodies
- Prosecution for offences
- Lawsuits
- Discipline by regulatory colleges and investigations by other oversight bodies
- Discipline by employers

Recent Amendments to *PHIPA*

Amendments to PHIPA proclaimed in force include:

- Privacy breaches meeting a threshold ***to be prescribed*** in regulation must be reported to our office; and
- Must also be reported by HICs to health regulatory colleges where a member of the College, who is employed, holds privileges or is affiliated with the HIC, has committed or is suspected of having committed a privacy breach.
- Fines have been doubled for offences from \$50,000 to \$100,000 for individual and \$250,000 to \$500,000 for organizations.
- Limitation period for prosecutions has been removed.



Health Information Custodians

Health Information Custodians (HICs) include:

- A health care practitioner who provides health care
- A person who operates a group practices of health care practitioners who provide health care
- A hospital, psychiatric facility and independent health facility
- A pharmacy, ambulance service, laboratory or specimen collection centre
- A long-term care home, care home for special care
- A community care access corporation
- A medical officer of health of a board of health
- Minister/Ministry of Health and Long-Term Care
- Canadian Blood Services



Agents

- An agent is a person that, with the authorization of a health information custodian, acts for or on behalf of the custodian in respect of personal health information
- An agent may include a person or company that contracts with, is employed by or volunteers for a custodian and, as a result, may have access to personal health information.
- A health information custodian remains responsible for the personal health information collected, used, disclosed, retained or disposed of by an agent

Duties Imposed on HICs and their Agents

- A number of duties are imposed on custodians and their agents under the Act
- These duties generally fall into four categories:
 - Collection, use and disclosure of PHI
 - Security of PHI
 - Responding to requests for access to, and correction of, records of PHI
 - Transparency of information practices

Collection, Use and Disclosure

- Not permitted to collect, use or disclose PHI...
 - if other information will serve the purpose
 - more than reasonably necessary
 - UNLESS
 - The individual **consents**
 - Permitted or required to be made without consent
- Providing PHI to an agent is considered a use by the custodian rather than a disclosure to the agent.

Harmonized Privacy Policies and Procedures Needed

Harmonized privacy policies & procedures should address:

- Privacy training
- Privacy assurance
(i.e. privacy readiness assessments)
- Logging, auditing and monitoring
- Consent management
- Privacy breach management
- Privacy complaints and inquiries management
- Access and correction

Safeguards

- Must ensure records of PHI are **retained, transferred** and **disposed** of securely
- Must take **reasonable steps** to ensure PHI is protected against
 - Theft, loss and unauthorized use or disclosure
 - Unauthorized copying, modification or disposal
- Must **notify individuals** at the first reasonable opportunity if PHI is stolen, lost or used or disclosed without authority

Transparency

- Custodians must **designate a contact person** responsible for compliance
- They must make available a **written public statement** that describes the custodian's information practices, including the **administrative, technical and physical safeguards** in place
- Written public statement must also include information about:
 - How to **contact** the custodian
 - How individuals can **access or correct** their records
 - How individuals can **complain** to the custodian and the IPC

GPEN Sweep: In-Home Medical Devices

GPEN SWEEP INDICATORS

INDICATOR 1: Do privacy communications adequately explain how personal information is COLLECTED, USED and DISCLOSED?

INDICATOR 2: Are users fully informed about how personal information collected by the device is STORED and has the company implemented SAFEGUARDS to prevent loss of data?

INDICATOR 3: Do privacy communications include CONTACT DETAILS for individuals wanting to contact the company about a privacy-related matter?

INDICATOR 4: Do privacy communications explain how a user can DELETE their information?

INDICATOR 5 (optional – only applies to PEAs who intend to contact DCs directly): Did the data controller provide a TIMELY, ADEQUATE and CLEAR response?



Electronic Service Providers

- An electronic service provider is a person who supplies services that enable a custodian to collect, use, modify, disclose, retain or dispose of personal health information electronically. If the electronic service provider is not an agent of the custodian, then it **shall not use** any personal health information to which it has access in the course of providing services to the custodian (except as necessary in the course of providing the service) and it **shall not disclose** the information.

Health Information Network Provider

- PHIPA contains requirements that apply to a specific type of electronic service provider, referred to as a health information network provider (HINP).
- A NIHP is a person who provides **services to two or more custodians**, where the services are provided primarily to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians.

HINP Requirements

Include a statutory duty to:

- notify the custodian of any **breaches**
- perform threat-risk and privacy impact **assessments**
- upon request, **provide** an electronic record to the custodian of all accesses and transfers of the personal health information
- ensure that retained **third parties** comply with necessary restrictions and conditions
- enter into a **written agreement** with the custodian
- make **publicly available** information about its services to the custodian.



IPC Guidance

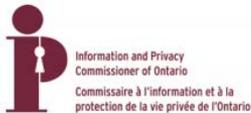
- PHIPA FAQ
- Manual for Review and Approval of Prescribed Persons and Entities
- Strong encryption
- Secure transfer of PHI
- Detecting and deterring unauthorized access
- Privacy impact assessments
- Cloud computing
- De-identification

PHIPA FAQ



Frequently Asked Questions Personal Health Information Protection Act

September 2015



Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Comprehensive guidance

- interpretation and application of *PHIPA*
- practices to protect PHI
- consent concerning PHI
- collection, use and disclosure of PHI
- fundraising and marketing
- research
- Ontario health cards and health numbers
- access to records of PHI and correction
- administration and enforcement

IPC Guidance

**MANUAL FOR THE
REVIEW AND APPROVAL
OF PRESCRIBED PERSONS
AND PRESCRIBED
ENTITIES**



Strong Encryption



Information and Privacy Commissioner of Ontario

Fact Sheet

Number 16
July 2010

Health-Care Requirement for Strong Encryption

The Office of the Information and Privacy Commissioner (IPC), in Order HO-004, and most recently in Order HO-007, required that health information be safeguarded at all times, specifically by ensuring that any personal health information stored on any mobile devices (e.g., laptops, memory sticks, PDAs) be strongly encrypted.¹ The Order did not otherwise define what constitutes “strong encryption” in the context of protecting the confidentiality, integrity, and availability of personal health information.

Accordingly, this paper provides a working definition of strong encryption and discusses the minimum functional and technical requirements of what may be considered to be strong encryption in a health-care environment. These, in turn, will provide procurement criteria that, if met, will ensure that personal health information stored on encrypted mobile devices or storage media will remain accessible to authorized users, but no one else.

Special thanks go to Dr. Robert Kyle, Durham Region Commissioner and Medical Officer of Health, for supporting the production of this paper.

Strong Encryption

Introduction

The term ‘strong encryption’ does not refer to a particular technical or design specification, or even to a specific encryption feature that could be inserted into a procurement or audit specification. No particular encryption technology — no matter how ‘strong’ it may be — can ever, by itself, ensure that information remains secure. Instead, a variety of circumstances and factors need to be taken into account to ensure that personal information is protected against access by unauthorized parties.

To begin with, a good encryption algorithm must be used — one that has been subjected to rigorous peer review. Next, the algorithm must be properly implemented. This may only be confirmed if the encryption system is tested by an independent security testing lab. Once the encryption system is deployed, the encryption keys must be protected and managed effectively. Users who are authorized to decrypt data must be securely authenticated by means of passwords, biometrics, or security tokens.

Other IPC Publications

- [No. 12 - Encrypting Personal Health Information on Mobile Devices](#)
Provides guidance to health information custodians on how to securely retain personal health information on mobile devices through encryption.
- [No.13 - Wireless Communication Technologies: Video Surveillance Systems](#)
Addresses privacy issues that arise from the use of wireless video surveillance technologies to transmit personal information and the proactive security measures required to protect the privacy of individuals.
- [No.16 - Health-Care Requirement for Strong Encryption](#)
Discusses the minimum functional and technical requirements of what may be considered strong encryption, thus ensuring that personal health information stored on mobile devices is protected.
- [No.18 - Secure Transfer of Personal Health Information](#)
Provides guidance for health information custodians on the secure transfer of records of personal health information.



Secure Transfer



Information and Privacy Commissioner of Ontario

Fact Sheet

Number 18
August 2012

The Secure Transfer of Personal Health Information

To ensure the timely and effective delivery of healthcare, health information custodians (custodians) may need to transfer personal health information. The need for vigilance in safeguarding the privacy of individuals during such transfers was highlighted when several courier packages sent by Cancer Care Ontario, containing the colon cancer screening information of more than 7,000 individuals, were lost. Following the loss, the Information and Privacy Commissioner of Ontario (IPC) ordered Cancer Care Ontario to stop transferring these records in paper format and to explore secure electronic means of transfer.¹ This Fact Sheet explains what this Order means for custodians.

Although the Order is directed at Cancer Care Ontario and was based on the particular circumstances at issue, it provides guidance that may help custodians minimize the risk of breaches when transferring records of personal health information. The Fact Sheet outlines a number of factors that should be considered by custodians in developing policies, procedures and practices for securely transferring records in paper and electronic format, recognizing that while

some custodians have embraced electronic records, for others it is a work-in-progress.

Order HO-011

Cancer Care Ontario used a courier service to transfer records containing colon cancer screening information to physicians in paper format after considering but rejecting other options, including transfers via a web portal or encrypted USB drives. It was later discovered that the colon cancer screening information of over 7,000 individuals had not been received by the physicians.

In reviewing this incident, the IPC considered the following factors:

- the characteristics of the person or organization transferring the records;
- the characteristics of the person or organization receiving the records;
- the number of individuals whose personal health information was contained in the records;
- the volume and frequency of the transfer(s); and

¹ Order HO-011

Safeguarding Privacy on Mobile Devices



www.ipc.on.ca

Detecting and Detering Unauthorized Access



Detecting and Detering
Unauthorized Access to
Personal Health Information



- Impact of unauthorized access
- Reducing the risk through:
 - Policies and procedures
 - Training and awareness
 - Privacy notices and warning flags
 - Confidentiality and end-user agreements
 - Access management
 - Logging, auditing and monitoring
 - Privacy breach management
 - Discipline

Privacy Impact Assessments (PIAs)



Planning for Success:
Privacy Impact Assessment
Guide



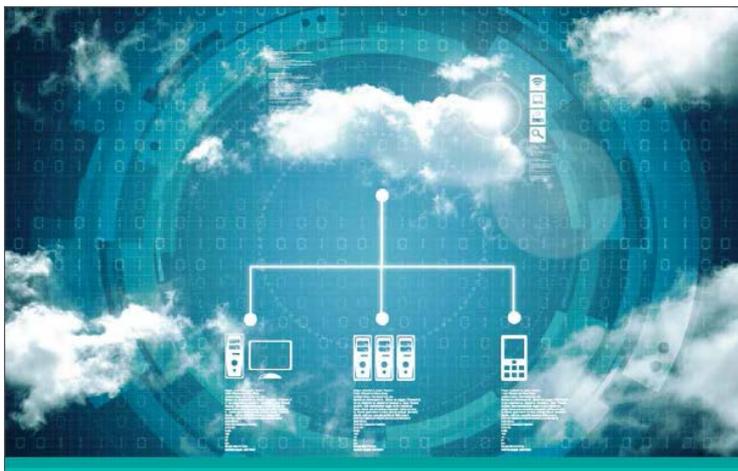
PIA Guide

- Tool to identify privacy effects, mitigate risks, of a given project
- Widely recognized as a best practice
- Simplified 4-step methodology with tools
- Basis for developing internal PIA policies and procedures

Download at: <https://goo.gl/9gM1x6>



Cloud Computing



Thinking About Clouds?
Privacy, security and compliance
considerations for Ontario public
sector institutions

February 2016

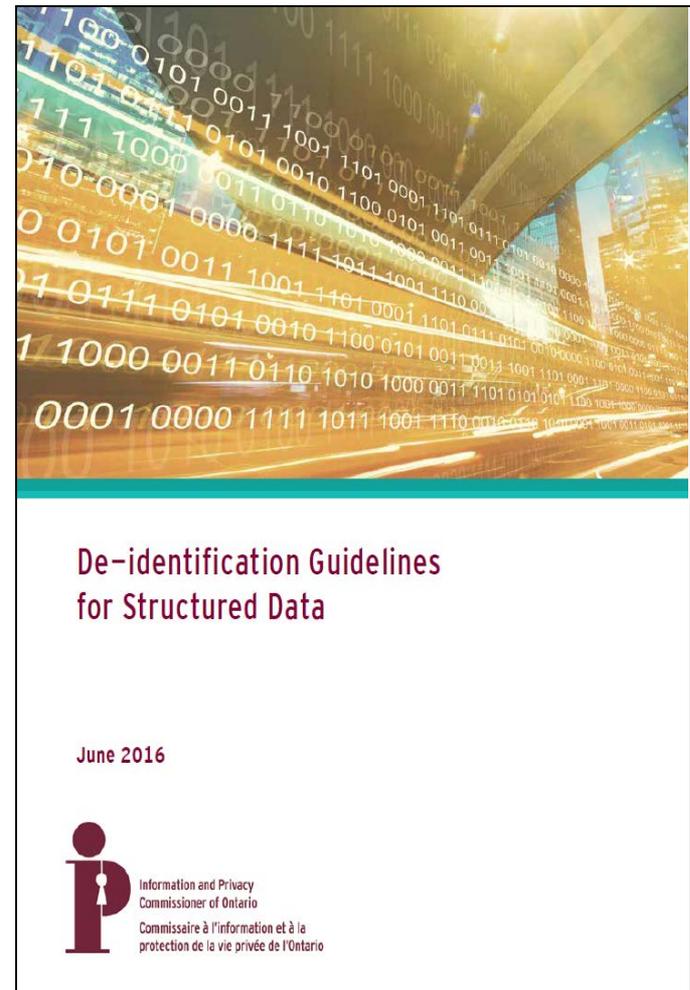


- Origins
- Definitions
- Identified Risks
 - Security
 - Privacy
 - Compliance
- Risk Mitigation Strategies



IPC Guidance on De-identification

- “De-identification” – the removal of personal information from a record or data set
- Provides a step-by-step process for de-identifying data sets
- Discusses key issues of:
 - direct and indirect (or “quasi-”) identifiers
 - types of re-identification attacks
 - common de-identification techniques
 - disclosures for open data and research
- Privacy protections do not apply to de-identified information



How to Contact Us

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965