



**Information Privacy Working Group (IPWG)  
Implementing Information  
Privacy and Security Training in Public Health**

**September, 2011**

**TABLE OF CONTENTS**

**PURPOSE**..... 1

**RATIONALE** ..... 1

WHY IS TRAINING NECESSARY? ..... 1

**SCOPE**..... 1

**CONTEXT** ..... 2

**PLANNING FOR TRAINING** ..... 3

**OUTCOMES OF TRAINING**..... 4

**SAMPLE LEARNING OBJECTIVES** ..... 5

**AUDIENCES**..... 5

WHO SHOULD USE THIS TRAINING STRATEGY? ..... 5

TARGET AUDIENCE/RECIPIENTS OF TRAINING ..... 5

**THE USE OF A COMPETENCY-BASED TRAINING APPROACH** ..... 6

WHAT ARE COMPETENCIES? ..... 6

WHY IS COMPETENCY-BASED TRAINING RECOMMENDED? ..... 7

**CONSIDERATIONS AND BEST PRACTICES** ..... 7

PLANNING ..... 7

IMPLEMENTATION..... 8

DELIVERY ..... 8

MEASURING EFFECTIVENESS ..... 8

REVISIONS ..... 9

**ASSUMPTIONS AND RISKS**..... 9

TRAINING DEVELOPMENT ASSUMPTIONS ..... 9

TRAINING DEVELOPMENT RISKS..... 9

**TRAINING CURRICULA** ..... 10

**CONCLUSION** ..... 10

**APPENDIX 1: CORE INFORMATION PRIVACY COMPETENCIES CHART**..... 11

**APPENDIX 2: POTENTIAL TRAINING MODULES** ..... 13

MODULE 1: INTRODUCTION TO PRIVACY, INFORMATION SECURITY AND CONFIDENTIALITY..... 13

MODULE 2: MFIPPA BASICS ..... 13

MODULE 3: PHIPA BASICS ..... 13

MODULE 4: PHIPA – CONSENT ..... 13

MODULE 5: PHIPA – COLLECTION AND USE OF PHI ..... 14

MODULE 6: PHIPA – DISCLOSURE OF PHI..... 14

MODULE 7: PRIVACY INCIDENTS AND BREACHES..... 14

MODULE 8: INFORMATION SECURITY – PHYSICAL SECURITY ..... 14

MODULE 9: INFORMATION SECURITY – ELECTRONIC SECURITY ..... 15

MODULE 10: INFORMATION SECURITY – WORKING OFF-SITE..... 15

MODULE 11: PHIPA – CIRCLE OF CARE AND PUBLIC HEALTH COMMUNITY OF PRACTICE..... 15

MODULE 12: PHIPA – ACCESS REQUESTS AND CORRECTION OF PHI ..... 15

MODULE 13: MFIPPA – FREEDOM OF INFORMATION (FOI) REQUESTS ..... 16

MODULE 14: MFIPPA – ROUTINE DISCLOSURE AND OPEN DATA ..... 16

MODULE 15: INTRODUCTION TO PRIVACY IMPACT ASSESSMENTS (PIAs) AND THREAT-RISK ASSESSMENTS (TRAs) ..... 16

MODULE 16: RESEARCH ETHICS BOARDS (REB)..... 16

**APPENDIX 3: SUPPORTIVE RESOURCES** ..... 17

**ACKNOWLEDGEMENTS** ..... 22

## Purpose

It is critical that all employees of public health units (PHUs) and other agents of local medical officers of health understand, internalize and act in accordance with their responsibility and accountability for the appropriate use and protection of personal health information (PHI). It is understood that training is a shared responsibility of both the employer and employee.

This training strategy, developed by the Information Privacy Working Group<sup>1</sup> (IPWG), is intended to foster and build consistency within and across Ontario's PHUs with respect to the collection, use, modification, disclosure, storage, and disposal of PHI by providing resources and highlighting best practices which may be built-upon and/or incorporated into PHU training plans. The strategy and associated curriculum are not exhaustive; customization, supplementation, and periodic updating will be required to meet changing local needs and issues.

**Note:** Throughout the training strategy, personal information is encompassed by the term *personal health information*<sup>2</sup>.

## Rationale

### *Why is training necessary?*

- Health Information Custodians (HICs) are mandated by the *Personal Health Information Protection Act, 2004* (PHIPA) to oversee and ensure the collection, use, disclosure, storage and disposal of PHI within their custody and control, and to take reasonable steps to ensure that all agents handle PHI in compliance with PHIPA.
- Similarly, the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) mandates the protection of personal information by municipal institutions, such as boards of health<sup>3</sup>.
- Training for public health staff and agents on information privacy is a best practice in ensuring the confidentiality and security of personal information and PHI in the custody and control of a HIC. Such training is vital to the meeting of *Public Health Organizational Standards* for effective information management.
- Information technology alone cannot ensure the protection or security of PHI. Administrative (e.g. policy), physical, and technical safeguards, and a staff culture of respect and good practice are also required.

## Scope

This training strategy provides high-level planning considerations, and is not tailored to any particular PHU's training needs for managing and protecting PHI. As such, it is imperative that each PHU identify its own requirements for the implementation of information privacy and security training, which may include but are not limited to:

- Determining training design and delivery, including training materials, logistics, facilities and technology requirements;
- Developing a communication strategy, including marketing of training program and modules;

---

<sup>1</sup> IPWG is jointly sponsored by the Ministry of Health and Long-Term Care (MOHLTC) and the Association of Local Public Health Agencies (aLPHa).

<sup>2</sup> Please see IPWG Fact Sheet #1 – Introduction to Personal Health Information.

<sup>3</sup> Be aware that the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection and Electronic Documents Act* exist and may be most familiar to non-health unit entities.

- Identifying and securing potential instructors for training modules; and,
- Measuring effectiveness of training and scheduling of updates and review of material.

Objectives include:

- Providing the rationale for the implementation of information privacy training within the PHU;
- Identifying some potential training objectives for the delivery of training to staff;
- Identifying potential learning outcomes for training participants;
- Providing key considerations and best practices for educating adults in a professional environment, taking into account the planning, implementation, delivery, measurement and feedback/revisions stages of implementing a training program and;
- Providing materials to assist PHUs with building and managing an in-house information privacy training program.

**Note:** This curriculum does not address professional practice standards issued by the health regulatory colleges, although it is expected that nothing in this strategy will conflict with professional practice requirements or training.

## Context

Health information custodians are responsible for ensuring that their agents are appropriately trained respecting the collection, use, modification, disclosure, storage, and disposal of personal health information.

Training is best undertaken in the context of a comprehensive policy and program respecting information privacy and security that would normally encompass the following:

1. Governance and Accountability:
  - PHU policies and practices that reflect and comply with legislative provisions (e.g., *Personal Information Protection Act* [PHIPA] and the *Municipal Freedom of Information and Protection of Privacy Act* [MFIPPA]) respecting information privacy and security;
  - Delegations of authority to agents including individuals identified as the Information Privacy Contact, associate medical officers of health, health unit executives, program managers, information and information technology managers and health unit staff.
2. Performance Management and Measurement:
  - These build on accountability and governance policies and practices to implement and ensure appropriate attitudes and behaviours respecting the collection, use, modification, disclosure, storage, and disposal of PHI. Continuous quality improvement (CQI) approaches are identified as a best practice to achieve the PHUs objectives respecting information privacy and security.
  - Performance management and measurement may address not only the effectiveness of PHU policies and practices, but also training provided to staff and other agents.
3. Risk Assessment and Mitigation:
  - A CQI best practice, this involves periodic reviews of the PHU's administrative, physical and technical policies and practices respecting information privacy and security.
  - Periodic assessment of training risks and mitigation strategies are also needed to address changes related to, for example, staff turn-over and technological evolution.
4. Enablers – such as Organizational Culture, Leadership and Training:

- Along with a culture that respects information privacy and leadership which models and reinforces the culture, *training* is a critical enabler to ensure buy-in and effective implementation and maintenance of information privacy and security policies and practices.
- Training enablers include marketing and outreach to staff and agents, in particular those who may not immediately identify that they have a role in information privacy and security.
- Training on information privacy and security should be aligned with and complement the PHU's administrative, physical and technical policies and practices.

## Planning for Training

Developing a training program for staff and other agents requires planning to ensure that the PHU's objectives are met in an effective and efficient manner. In addition, consider the need for a general orientation to information privacy and security in a public health context for members of the board of health.

Below are some considerations for the planning and development stage of a training program.

1. Identify and assess existing information privacy policies, tools and strategies. Assessments should be undertaken periodically, especially if changes are made to equipment and information privacy policies or procedures.
  - Does the existing staff training plan include information privacy and security?
  - If YES, does the training reflect current information privacy policies and practices as well as anticipated risks? If new policies, practices or technology have been adopted, what changes (if any) are required?
2. Identify potential opportunities to improve employees' compliance with information privacy and security measures and procedures within the PHU.
  - Have challenges or risks respecting information privacy and security been identified or experienced (e.g. privacy incidents, breaches or possible exposure to such)?
  - If YES, what policy and/or process changes (if any) are needed to enable the PHU to prevent future challenges and mitigate anticipated risks?
3. Identify resources that may be required to renew your training plan to better reflect current information privacy requirements and risks.
  - Are additional learner and/or instructor materials required? Are expert instructors needed? Do new physical and hardware changes to meet information privacy requirements require additional or revised training and/or training materials or resources?
  - If YES, how will financial and human resources be allocated to meet the requirements?
4. Establish training delivery methods that are best suited for the size and capacity of the PHU.
  - Do certain employees have particular training and learning needs? Does the PHU have the equipment, technology and space available to offer variety in training delivery? Does the diversity of employment within the PHU warrant separate training groups (e.g., are separate groups required for the family health and tobacco use control teams)?
  - Are appropriate training leaders or facilitators (i.e., instructors who are knowledgeable about the subject matter) available or accessible?

- Is the time planned and/or available for each proposed training session appropriate or sufficient? If not, how can the needed time be secured?
5. Determine the PHU's objectives for implementing or augmenting information privacy training.
    - Will training be directed to new employees and/or existing employees? What are the training needs of these groups (e.g., full orientation or updating re new information privacy requirements)?
    - Are changes to employees' knowledge, attitudes and/or behavioural competencies needed?
    - If YES, what specific changes are required and how will the appropriate knowledge, attitudes and/or behaviour be transferred to and retained by the PHU staff?
  6. Build in promotional strategies to engage staff and capture their attention.
    - What opportunities and vehicles exist to communicate with staff? Are there particular opportunities (e.g., general staff meetings) at which information privacy and security information can be provided? What are the incentives for staff participation?
    - What key messages are required and who should deliver these messages?
    - Strategies may also be required to engage members of the board of health.

## Outcomes of Training

Identifying potential outcomes and measuring the effectiveness of training are key components of incorporating a training strategy within a performance management framework. Below are some possible outcomes of training.

1. Training supports and is aligned with the PHU's policies and procedures for information privacy.
  - Training communications match the PHU's policies and protocols.
  - Training program addresses gaps in current practices or behaviours.
2. PHU staff should be able to take a proactive rather than reactive role in protecting PHI.
  - Are staff are equipped to manage and protect PHI in accordance to PHIPA and the PHU's information privacy policies?
  - Staff are able to identify and appropriately respond to potential privacy concerns.
3. Information privacy and security become part of the current organizational culture.
  - Staff actively engages in desired privacy behavioural patterns throughout the information management lifecycle.

## Sample Learning Objectives

While learning objectives may vary among PHUs, in general, training participants should be able to:

- Identify and understand the principles of individual privacy and confidentiality; the definitions of confidential information, personal information, personal health information; and the concepts of information privacy and personal information protection and security.
- Describe why protecting personal health information is important to individuals, their employers, the public, government institutions, and themselves.
- Describe the basic concepts of collection, use and disclosure of PHI, and the role of consent, as agents of the HIC.
- Describe legal and policy requirements for the protection of PHI within Ontario and their work environment.
- Know the key privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), and the *Personal Health Information Protection Act* (PHIPA).
- Explain and implement some basic safeguards (administrative, physical and technological) to protect personal information, including key safeguards mandated by their employer.
- Know how to recognize a potential privacy incident or breach and apply organizational procedures respecting the mitigation and management of the incident and/or breach.
- Explain the right of access provided in the legislation and the process of responding to an access request.
- Know how the legal and policy provisions can be applied to real situations in their workplace.

## Audiences

### ***Who should use this Training Strategy?***

- Health information custodians;
- Privacy officers and/or designated information privacy contact persons;
- Program managers;
- Information Technology (IT) managers/administrators;
- Others exposed to personal and personal health information.

Also consider whether a general orientation to information privacy and security is required for board of health members.

### ***Target Audience/Recipients of Training***

Agents of the Health Information Custodian (HIC)

- PHU<sup>4</sup> staff (e.g., regulated and unregulated health staff, including public health inspectors, health promoters, epidemiologists, planners, and volunteers.);
- Contracted staff performing duties on behalf of the HIC (e.g., medical locums, data destruction/disposal suppliers; etc.);
- Administrative and financial support staff;
- Resident Information and Information Technology (I & IT) support and records management (including data administration) staff;
- Public Health Program Managers and Directors;

---

<sup>4</sup> PHU staff includes staff assigned to the Board of Health/PHU by a municipality.

- Researchers (e.g., those conducting research on behalf of the HIC and those undertaking independent research projects using PHU data);
- Municipal employees working with or on behalf of the PHU; and,
- Contracted I & IT support and records management contractors (e.g., IT service providers, records storage, maintenance and disposal companies).

## The use of a Competency-based Training approach

### ***What are competencies?***

Information privacy competencies are the essential knowledge, skills and attitudes required to effectively safeguard PHI. They are not limited to the boundaries of specific disciplines and are independent of program and topic.<sup>5</sup> Competencies can be measured and compared to a defined standard. Competencies can also be developed and improved by training.

The use of competency-based training for information privacy and security facilitates identification of competencies that are needed to perform a variety of functions related to collecting, using, managing, disposing of and protecting PHI, and to assist employees with acquiring, maintaining, improving and assessing their proficiency respecting these functions.

In this training strategy, we have identified some key information privacy competencies, as well as three levels of proficiency for each competency. Please refer to *Appendix 1: Core Information Privacy Competencies Chart* for managing and protecting PHI. The following competency levels are identified:

- **Awareness** – This competency level is appropriate for staff with minimal access to PHI and other types of confidential information in their daily work. Staff at this level would be able to identify the confidential nature of information; would follow clearly stated rules when handling routine PHI tasks (e.g., processing PHI data, administering a disclosure); and would seek advice and guidance from knowledgeable senior staff to respond to/address non-routine situations. PHUs should consider training all staff to a minimum competency level of awareness for all the competencies.
- **Knowledgeable** – This competency level is appropriate for staff with routine access to and program-specific responsibility for PHI and other types of confidential information. Staff at this level would be able to recognize confidential information/data and understand the individual and organizational consequences of inappropriate or unauthorized use; would be able to extrapolate from general policies/practices to non-routine situations; and would be able to anticipate information privacy issues and make use of situational experience to assess and respond to non-routine or precedent-setting situations. Some examples of roles that may require training to the competency level of knowledgeable are public health inspectors and nurses, epidemiologists, program managers, and all administrative and/or data management staff that routinely handle or access PHI.
- **Proficient** – This competency level is appropriate for staff with extensive access to and/or responsibility for PHI and other types of confidential information. Staff at this level would be able to: recognize confidential information/data; comprehend the personal and organizational consequences of inappropriate or unauthorized use; apply principles and implement knowledge to evaluate and solve problems; and supervise, lead and/or serve as an expert in managing privacy issues. Some examples of roles that may require

---

<sup>5</sup> Adapted from Public Health Agency of Canada (2007), Core competencies for Public Health in Canada: Release 1.0

training to the “proficient” competency level are the Medical and Associate Medical Officers of Health, Chief Nursing Officer/Senior Nurse Leader, privacy officers or contact persons, and I & IT management.

### ***Why is competency-based training recommended?***

Each staff member may have a different interaction with PHI, which may require employment of various privacy competencies. Identifying the privacy competencies needed to effectively manage and protect PHI allows for:

- Setting expectations for staff members regarding their familiarity with information privacy and security management procedures;
- Tailoring of training for different types of job functions;
- Training for both general and specific situations that an employee may encounter in their role;
- Re-training as new policies are implemented; and/or
- Re-training as employees change jobs.

For staff members who may wish to become information privacy professionals, higher level training and certifications are available. The IPWG proposes that PHUs strive to train core program staff to the “knowledgeable” level of competency. The “proficient” level may be beyond the scope of internal training and may be better achieved through external privacy professional training.

## **Considerations and best practices**

### ***Planning***

- It is important to identify and meet the needs of potential users of PHI, as various employee groups will have different relationships with managing PHI.
  - Identification of skill/knowledge/attitude gaps with current staff will assist in determining which area requires specific and immediate attention.
- While it is important to meet individual training and learning needs, it is equally important to ensure that training meets organizational needs. In other words, PHU staff need to understand the organization’s overall strategy and comply with policies and protocols for the protection and security of PHI.
  - Training program objectives must also reflect the organization’s objectives. Objectives should also be focused and practical in nature.
- The success of training strategies requires buy-in from all organizational levels, especially active support from senior leaders, as well as an understanding of the organizational culture within the PHU and barriers to change. Where boards of health are embedded in a municipal organization, support from the host organization is also critical.
- It is important to develop a targeted communication campaign to promote the training to desired participants. Training program goals, objectives and expectations also need to be clearly communicated to participants to foster understanding of why they are participating and how they will benefit from participation.
- Training also requires commitment of resources and effort (e.g., time). Managers need to provide both time and support to ensure a favourable organizational culture.
- It is important to consider the size (the number of employees) and capacity (organizational resources) of the organization when developing the training program. It

may be necessary to seek outside resources to develop and deliver the training program.

- Training sessions should outline or include a discussion of:
  - The material to be learned and its significance;
  - The skills or competencies needed to effectively apply the learning to on-the-job situations;
  - The behavioural changes that will allow for adoption of the new procedures, and what the behaviour should look like;
  - Known or anticipated barriers to change and possible ways to overcome them; and
  - The organization's expectations regarding future application of subject materials.

### ***Implementation***

- Information privacy and security training should be incorporated into new-hire orientation for staff (including contract positions and volunteers) within the PHU.
- Periodic training for existing staff to refresh knowledge, skills and attitudes is a best practice.
- Regular and continuous review of training material should be a part of a comprehensive training plan.
- Staff sign-offs for reviewing material provides a measure of accountability.
- Making managers accountable for staff training (e.g. ensuring that managers' performance plans or agreements include a measure of their staff's compliance with information privacy training) is a key accountability tactic.

### ***Delivery***

- Communication from senior leadership to staff highlighting the importance of information privacy and security is a best practice – senior leaders should instil respect for information privacy and security among staff and model appropriate attitudes and behaviours.
- Offering a variety of learning vehicles (e.g., workshop format, one-on-one training, individual study, practice scenarios, simulations, e-learning modules) will allow employees to choose the most suitable mode for their learning.
- Incorporating real life applications to the participants' job functions and work environment, and employing real life examples of how the information is applicable to them fosters understanding, retention and desired behaviour change. Interactive programs are a best practice.
- The use of experienced instructors (internal or external) will encourage buy-in and build confidence in the implementation of the training.
- The use of simulation scenarios would give employees an opportunity to practise applying their newly learned skills and/or behaviour prior to using them in a real-situation.
- Staff recognition for participation and achievement is appreciated by staff.

### ***Measuring Effectiveness***

- Pre-testing before training (in combination with post-training testing) could be considered to identify the level and amount of skill, attitude or behaviour change that may have occurred because of the training. Pre-testing also provides an opportunity to identify preferred learning styles and vehicles.
  - To understand the effectiveness of a training program, the skills and/or knowledge level of each individual trainee should be assessed prior to participation. Assessment

can be simple and quick to get a sense of where the trainee is starting and gaps in attitude and/or understanding.

- Post-training testing in a manner that allows the participants to display their learning and understanding of the material (e.g. written and/or verbal tests, analyzing case studies, mock simulations, and developing presentations) is a best practice to gauge whether the training material has made an impact on the participants' skill and/or competency level, attitudes or behaviour.
- Obtaining post-training feedback from staff will identify additional needs for training, as well as reinforce the material learned.
- Periodic self-report assessments, on-the-job observation, and employee performance appraisals can be used as tools to assess the relationship between training and job performance.
- Establishing management accountability for training facilitates participation by team members.

### **Revisions**

- Taking note of "lessons learned" throughout the stages of implementation will identify successes and potential challenges, and allow for a smoother implementation of revisions to training methods.
- Taking note of "lessons learned" on the job may provide additional scenarios that could be included in future training.

## **Assumptions and Risks**

### ***Training Development Assumptions***

- Information privacy and security training can be incorporated into existing general organizational training strategies.
- Training messages and communications align with information privacy policies and protocols.
- The PHU is responsible for determining which role-based competency level is adequate for its staff.
- The HIC and/or corporate and program managers are responsible for identifying priority groups for training.
- Training may need to be phased over a number of work cycles or among staff groups.
- The PHU is responsible for deciding to implement employee recognition for those who have increased their level of competency,
- IPWG Tool Kit resources are available to PHUs electronically.
- Materials should comply with Accessibility for Ontarians with Disabilities Act (AODA) requirements and, as appropriate, be available in English and French.
- Existing resources should be used where appropriate and practical, and updated and supplemented when required.

### ***Training Development Risks***

- Organizational overconfidence – training is rarely a one-time event and may have to be repeated and reinforced.
- Training implementation and delivery should reflect the PHU's organizational culture.
- Training strategies need to address cohort changes and staff turnover.
- Some aspects of the training curriculum may undergo an evergreen process as resources and technologies evolve. Protocols outlining the evergreen process may need to be developed.

## Training Curricula

The sample curriculum outlined in this Training Strategy is rooted in the best practice of using the Information Management Lifecycle (e.g., collection, use, modification, transfer (including transportation), disclosure, retention and/or disposal) and the Fair Information Principles to manage and protect PHI. These concepts are also linked to the *Personal Health Information Protection Act* (PHIPA). The curriculum is designed to align all three concepts in a concise manner, as well as address PHI privacy and security challenges (e.g. use of mobile devices).

*Appendix 2: Potential Training Modules* provides a general curriculum for information privacy and security training broken down into training modules. PHUs should review and revise the curriculum and training modules from the perspective of their training needs and information privacy and security risk assessment, and revise the modules appropriately. In particular, opportunities to build in their own information privacy and security policies and protocols should be found and implemented.

Please also review the IPWG's Information Privacy and Security Tool Kit to identify resources that may be able to supplement your information privacy and security training curriculum and resources.

## Conclusion

The purpose of this Training Strategy is to assist PHUs in developing and building comprehensive training programs relating to PHI privacy and security. The content and associated resources are not exhaustive, and many health-related organizations have developed information privacy and security training resources that may be applicable, with some adaptation, to the public health context. Additionally, there is much to be learned from non-health organizations that face similar challenges to sensitive or confidential information within their custody and control.

The IPWG encourages both exploration of these resources to identify best practices and useful training materials, and the sharing of such findings within the public health family.

## APPENDIX 1: Core Information Privacy Competencies Chart

**Purpose:** To identify basic competencies<sup>6</sup> for public health staff working with personal health information (PHI)<sup>7</sup> for the purpose of providing provincial-level training support to PHUs. The competencies are not intended to replace any knowledge or skill requirement associated with job descriptions or task assignments. The general intention is to assist staff with applying discretion, exercising judgement and considering options when dealing with PHI.

A progressive model can be used when determining the knowledge and/or skill level of staff prior to and during training. With more exposure to, and experience with handling PHI, in addition to regular training, staff may progress from an awareness and recognition level for any particular competency, to an application and assessment level. The progression from one level to the next would also depend on job role.

COMPETENCY	DESCRIPTORS OF COMPETENCY
Identification of PHI	<ul style="list-style-type: none"> <li>▪ Ability to recognize what constitutes personal health information (PHI) and other identifiable confidential information, and the documents that contain PHI (patient records, faxes, intake forms, iPHIS).</li> <li>▪ Awareness of organizational procedures respecting the handling of PHI.</li> </ul>
Knowledge and application of privacy legislation, the Information Management Lifecycle and the Fair Information Practices	<ul style="list-style-type: none"> <li>▪ Familiarity with and application of the <i>Personal Health Information Protection Act</i> (PHIPA) and the <i>Municipal Freedom of Information and Protection of Privacy Act</i> (MFIPPA) to daily business.</li> <li>▪ Ability to manage PHI in day-to-day activities.</li> <li>▪ Familiarity with the information management lifecycle within the organization.</li> <li>▪ Understanding of the Fair Information Practices and how they may apply to job-related activities and situations.</li> <li>▪ Ability to recognize the personal and organizational responsibility respecting the protection and appropriate use of personal health information.</li> </ul>
Knowledge and application of organizational and procedural protocols respecting PHI	<ul style="list-style-type: none"> <li>▪ Ability to recognize and apply organizational procedures respecting the collection, transmission, transport, storage, retention, and disposal of PHI.</li> <li>▪ Ability to maintain accurate, complete, and up-to-date records containing PHI and other confidential information.</li> </ul>

<sup>6</sup> Also see: Public Health Agency of Canada (2007), Core competencies for Public Health in Canada: Release 1.0. Retrieved from <http://www.phac-aspc.gc.ca/ccph-cesp/pdfs/cc-manual-eng090407.pdf>.

<sup>7</sup> Personal health information refers to oral or written information about the individual's health status or information related to the provision of health care for that individual. For the expanded definition, please refer to the *Personal Health Information Protection Act*. Personal health information includes identifying information that would be considered to be personal information as described in *Municipal Freedom of Information and Protection of Privacy Act*

COMPETENCY	DESCRIPTORS OF COMPETENCY
Comprehension of consent types and application of requirements relating to the collection, use, and disclosure of PHI as defined in PHIPA	<ul style="list-style-type: none"> <li>▪ Comprehension and application of the legislative requirements surrounding consent such as elements of valid consent; types of consent; authorization for consent; limiting and/or withholding consent; and recognition of situations where consent is required.</li> <li>▪ Knowledge of different types of consent required for daily practice and ability to identify whether appropriate consent has been achieved.</li> <li>▪ Understanding of circumstances that require additional information or direction respecting securing appropriate consent.</li> </ul>
Comprehension and application of principles and requirements for collection, use and disclosure of PHI	<ul style="list-style-type: none"> <li>▪ Ability to comprehend and apply legislative provisions and organizational policies respecting the collection, use, disclosure, retention and storage of PHI, including access requests.</li> <li>▪ Ability to exercise discretion when applying legislative permissions and limitations to the collection, use and disclosure of PHI.</li> </ul>
Comprehension and application of principles and practices for safeguarding PHI and dealing with privacy incidents	<ul style="list-style-type: none"> <li>▪ Understanding and application of organization's administrative, technical and physical safeguards to protect PHI.</li> <li>▪ Ability to monitor and ensure appropriate use of PHI safeguards by team members.</li> <li>▪ Ability to recognize, assess and mitigate risks of a privacy incident in daily and/or organizational practices.</li> <li>▪ Comprehension and application of procedures for reporting potential privacy incidents.</li> <li>▪ Ability to effectively manage a privacy incident.</li> </ul>

## APPENDIX 2: Potential Training Modules

Below is an example of a modular training curriculum developed by Toronto Public Health<sup>8</sup>, with modifications suggested by the IPWG's review. The order of delivery of training modules can be changed to meet organizational and learner needs.

### ***Module 1: Introduction to Privacy, Information Security and Confidentiality***

- What is privacy? – 10 principles.
- What is confidentiality? How does it affect you/your job?
- What is information security?
- How do these interact?
- What are the key differences between them?
- What are the drivers for each – legislative, policy, best practice, etc.?
- What is your role?

### ***Module 2: MFIPPA Basics***

- Overview of the legislation
- Goals and purposes
- What does it cover?
- What is personal information?
- What policies and procedures are in place to support application of the legislation?
- Roles and responsibilities under MFIPPA
- Role of the Information & Privacy Commissioner.

### ***Module 3: PHIPA Basics***

- Overview of the legislation.
- What is personal health information (PHI)?
- Key PHIPA principles
  - Consent
  - Collection of PHI
  - Use of PHI
  - Disclosure
  - Access to and correction of PHI
- Health Information Custodians and Agents
  - What is your role and obligations?
- Substitute Decision-makers
- Information practices statement
- Research Ethics Boards (REBs)
- Role of the Information & Privacy Commissioner.

### ***Module 4: PHIPA – Consent***

- Basics of consent.
- Types of consent.
- Express versus Implied consent;
- Public Health Community of Practice<sup>9</sup>;

---

<sup>8</sup> Toronto Public Health. Quality Assurance Advisory Committee, Privacy, Security and Confidentiality Curriculum, as adapted.

- Circle of Care<sup>10</sup>.
- When is expressed consent required?
  - Assessing consent received.
- When is consent not required?
- What is your role?

#### **Module 5: PHIPA – Collection and Use of PHI**

- Principles underlying collection and use of PHI.
- Limiting collection and use of alternative data.
- Primary and secondary uses.
  - Identifying and clarifying uses of PHI.
  - Program monitoring, program evaluation, program planning and research.
- Obtaining or ensuring that appropriate consent is in place.
- Overview of Privacy Impact Assessment.
  - Policies and procedures for use of PHI.
  - Research Ethics Boards – role and approvals.

#### **Module 6: PHIPA – Disclosure of PHI**

- Principles underlying disclosure of PHI.
- Consent to disclosure.
- What is your role?
- Policies and procedures for disclosure.
- Unauthorized or inappropriate disclosures.
  - Identifying a possible privacy incident or privacy breach.
  - Receipt of unauthorized or inappropriate disclosure.
- Best practices in providing disclosure.
- Best practices in receiving disclosure.

#### **Module 7: Privacy incidents and Breaches**

- What is a privacy incident or lapse?
- What is a privacy breach?
- Potential consequences of a privacy incident or breach.
- What are requirements under MFIPPA and PHIPA?
- How to handle a privacy incident or breach:
  - Internal notification
  - Stopping the breach
  - Remediation
  - Other notifications.
- Roles of the [PHU] Privacy Officer, management and staff.
- Role of the Information & Privacy Commissioner (IPC).

#### **Module 8: Information Security – Physical Security**

- Role of physical security.
- Premises – access control.
- Workspaces.

---

<sup>9</sup> Information Privacy Working Group (August 2011), *Fact Sheet #21: Considerations for Responding to Requests for Use, Disclosure or Access to Personal Health Information*.

<sup>10</sup> Information and Privacy Commissioner of Ontario. *Circle of Care – Sharing Personal Health Information for Health Care Purposes*. <http://www.ipc.on.ca/images/Resources/circle-care.pdf>

- On-site storage – desks, filing cabinets.
- Secure destruction of paper.
- Security audits.

### ***Module 9: Information Security – Electronic Security***

- Role of electronic security.
- Access controls – network, e-mails (work and personal e-mails), data bases.
  - PHU Policies and Practices.
  - Role of corporate information and information technology resources.
- Passwords.
  - Creating strong passwords.
  - Policies regarding sharing passwords.
- Mobile devices and media.
  - Policies respecting use of mobile devices and media.
- Role of encryption.
- Faxing – when and how.

### ***Module 10: Information Security – Working Off-Site***

- PHU policies and procedures for working off-site and from home.
- Policies and procedures for working from home.
  - Ending electronic data to home computers.
  - VPNs.
- Secure transportation.
  - Mobile media (USB Keys) and devices (laptops).
  - Encryption.
  - Uploading to home system.
- Secure storage.
  - Mobile media and devices.
  - Encryption.
- Reporting loss of mobile devices or media – policies and procedures.
- Best practices for working off-site.

### ***Module 11: PHIPA – Circle of Care and Public Health Community of Practice***

- What is a “circle of care” and “public health community of practice”?
- Assumed implied and expressed consent.
- Who can rely on assumed implied consent under PHIPA?
- What is required in order for a HIC to assume implied consent?
- Circle of Care and Community of Practice at PHU.

### ***Module 12: PHIPA – Access Requests and Correction of PHI***

- What is an access request?
  - Principles.
  - How is it different from disclosure?
- Who may request access to PHI?
  - Legislative requirements.
- Who may correct PHI?
  - Policies and procedures for correcting PHI.
- Formal requests versus informal requests.
- Role of substitute decision-makers and other agents.
- Tracking and documenting requests and corrections.

**Module 13: MFIPPA – Freedom of Information (FOI) Requests**

- What is an FOI request?
- Legislative requirements, timelines.
- Exemptions.
- Extensions.
- PHU policies and procedures to support compliance with MFIPPA.
- Severing of information.
- Role of program managers/privacy officers in supporting responses to FOI requests.

**Module 14: MFIPPA – Routine Disclosure and Open Data**

- What is routine disclosure and open data?
- How it supports FOI and open government.
- What is routinely disclosed by the PHU?
- How to handle routine disclosure requests.
- Overview of “open data” initiatives.

**Module 15: Introduction to Privacy Impact Assessments (PIAs) and Threat-Risk Assessments (TRAs)**

- What is a PIA?
- What is a TRA?
- What do they achieve?
- Why are they necessary?
- Who are they undertaken?
- Link to collection, use and disclosure of PHI.
- Link to research ethics boards.

**Module 16: Research Ethics Boards (REB)**

- What is a Research Ethics Board?
- Why are REBs necessary?
- Composition of an REB.
- Role of an REB.
- What is a research plan?
- Research Ethics clearance at PHU
  - Policies, procedures and timelines

## APPENDIX 3: Supportive Resources

Training and reference materials are included from a variety of organizations including contributing health units. When possible, resources are adapted to reflect public health priorities. Please also review the IPWG's Information Privacy Tool Kit.

**Note:** IPWG – Information Privacy Working Group; IPC – Information and Privacy Commissioner for Ontario.

Curriculum Topics	Notes	Available Training Resources
Introduction to Personal Health Information	<ul style="list-style-type: none"> <li>▪ Definitions of basic terms such as personal and personal health information, confidential information, etc.</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #1: Introduction to Personal Health Information</i></li> <li>▪ Media Awareness Network: <i>Your guide to the CSA's Privacy Code</i>: <a href="http://www.media-awareness.ca/english/resources/educational/handouts/privacy/csa_privacy_code_guide.cfm">http://www.media-awareness.ca/english/resources/educational/handouts/privacy/csa_privacy_code_guide.cfm</a></li> <li>▪ Toronto Academic Health Science Network Research Ethics Committee. <i>Principles For Development Of Policy And Guidelines on Security of PHI Used for Research Purposes</i>, Appendix 2</li> <li>▪ Ontario Hospital Association: <i>Hospital Privacy Toolkit</i>: <a href="http://www.oha.com/KnowledgeCentre/Library/Toolkits/PublishingImages/Hospital%20Privacy%20toolkit.pdf">http://www.oha.com/KnowledgeCentre/Library/Toolkits/PublishingImages/Hospital%20Privacy%20toolkit.pdf</a></li> <li>▪ MOHLTC Public Health Practice Branch Town Hall: <i>Personal Information and You</i></li> </ul>
Overview of Privacy Legislation	<ul style="list-style-type: none"> <li>▪ Understanding the legislative provisions concerning PHI (i.e. MFIPPA, PHIPA).</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #2: Overview of Privacy Legislation</i></li> <li>▪ IPWG. <i>Fact Sheet #3: Key Legislative Requirements for Public Health Units</i></li> <li>▪ IPWG. <i>Fact Sheet # 10: Key Privacy Principles for Collecting, Using and Disclosing Personal Health Information</i></li> <li>▪ <i>Personal Health Information Protection Act (PHIPA)</i>: <a href="http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p_03_e.htm">http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p_03_e.htm</a></li> <li>▪ <i>Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)</i>: <a href="http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm">http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm</a></li> <li>▪ Public Health Ontario. <i>Privacy Management Model (presentation)</i></li> <li>▪ Access and Privacy Workshop (2006). <i>M/FIPPA/PHIPA Interaction Issues: One Year Later</i></li> </ul>
Key legislative principles of PHIPA relating to Public Health	<ul style="list-style-type: none"> <li>▪ Overview of the key requirements and responsibilities of PHIPA</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #3: Key Legislative Requirements for Public Health Units</i></li> <li>▪ IPWG. <i>Fact Sheet # 10: Key Privacy Principles for Collecting, Using and Disclosing Personal Health Information</i></li> <li>▪ Durham Region Health Department. <i>Privacy Policy</i>: Appendix A</li> <li>▪ Ontario Medical Association: <i>Ontario MD Privacy and Security (presentation)</i>:</li> </ul>

Curriculum Topics	Notes	Available Training Resources
		<ul style="list-style-type: none"> <li>▪ <a href="https://www.ontariomd.ca/imageserver/OMDContent/privacy_encryption/PrivacyEncryption.htm">https://www.ontariomd.ca/imageserver/OMDContent/privacy_encryption/PrivacyEncryption.htm</a></li> <li>▪ Information and Privacy Commissioner of Ontario (IPC). A Guide to the <i>Personal Health Information Protection Act</i>. <a href="http://www.ipc.on.ca/images/Resources/hguide-e.pdf">http://www.ipc.on.ca/images/Resources/hguide-e.pdf</a></li> </ul>
Roles and Responsibilities	<ul style="list-style-type: none"> <li>▪ Understanding of requirements of the health information custodian (HIC), designated contact person and agents of the HIC</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #4: Roles and Responsibilities of the Health Information Custodians, Contact Persons and Agents</i></li> <li>▪ Durham Region Health Department. <i>Privacy and Security Training</i> (presentation)</li> <li>▪ College of Nurses of Ontario: <i>Guide to Privacy Requirements and Policies for Nurses</i></li> </ul>
Accountability, identifying purposes and openness	<ul style="list-style-type: none"> <li>▪ Linking job-related functions to these Fair Information Principles and PHIPA</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #5: Accountability, Identifying Purposes, and Openness</i></li> <li>▪ Region of Waterloo Public Health Policy and Procedure Manual: <i>Accountability, Delegation of Authority</i></li> <li>▪ Durham Region Health Department. <i>Privacy Policy: Accountability and Identifying Purposes</i></li> <li>▪ Information and Privacy Commissioner of Ontario. <i>Your Health Information...in our facility</i>. <a href="http://www.ipc.on.ca/images/Resources/up-1BrochFacility.pdf">http://www.ipc.on.ca/images/Resources/up-1BrochFacility.pdf</a></li> </ul>
Consent	<ul style="list-style-type: none"> <li>▪ Types of consent and understanding the consent requirements and limitations and how they affect daily practice</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #6: Considerations for Consent</i></li> <li>▪ College of Nurses of Ontario: <i>Confidentiality and Privacy Personal Health Information</i></li> <li>▪ York Region Community and Health Services Department: <i>Notice of Privacy and Information Practices</i></li> <li>▪ Niagara Region Public Health. <i>Privacy Policy</i>, Appendix 50</li> <li>▪ IPC. <i>Fact Sheet: Lock Box Fact Sheet</i>: <a href="http://www.ipc.on.ca/images/Resources/fact-08-e.pdf">http://www.ipc.on.ca/images/Resources/fact-08-e.pdf</a></li> </ul>
Limiting the collection, use, and disclosure of PHI	<ul style="list-style-type: none"> <li>▪ Understanding the key limitations respecting the collection, use and disclosure of PHI and the importance of discretion</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet # 7: Considerations for Limiting the Collection of Personal Health Information</i></li> <li>▪ IPWG. <i>Fact Sheet #8: Considerations for Limiting the Use and Disclosure of Personal Health Information</i></li> <li>▪ IPWG. <i>Fact Sheet #9: Disclosure Required by Law</i></li> <li>▪ IPWG: <i>Fact Sheet # 10: Key Privacy Principles for Collecting, Using and Disclosing Personal Health Information</i></li> <li>▪ IPC: <i>FAQ – Health Cards and Health Card Numbers</i>: <a href="http://www.ipc.on.ca/images/Resources/hfaq-cards-e.pdf">http://www.ipc.on.ca/images/Resources/hfaq-cards-e.pdf</a></li> <li>▪ IPWG. <i>Fact Sheet #21: Considerations for Responding to Requests for Use, Disclosure or Access to Personal Health Information</i></li> </ul>

Curriculum Topics	Notes	Available Training Resources
Collection, use, and disclosure of PHI	<ul style="list-style-type: none"> <li>▪ Understanding of the provisions for collection, use and disclosure of PHI, understanding the difference between collection, use and disclosure, and considerations for research</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #8: Considerations for Limiting the Use and Disclosure of Personal Health information</i></li> <li>▪ IPWG. <i>Fact Sheet #9: Disclosure Required by Law</i></li> <li>▪ IPWG: <i>Fact Sheet # 10: Key Privacy Principles for Collecting, Using and Disclosing Personal Health Information</i></li> <li>▪ IPWG. <i>Fact Sheet #15: Personal Health Information Transmittal via Fax</i></li> <li>▪ IPWG. <i>Fact Sheet #17: E-Mail and Personal Health Information</i></li> <li>▪ Region of Waterloo Public Health. <i>Policy and Procedure Manual: Disclosure of PHI to Law Enforcement Agencies</i></li> <li>▪ Region of Waterloo Public Health. <i>Policy and Procedure Manual: Research Activities using PHI</i></li> </ul>
Retention	<ul style="list-style-type: none"> <li>▪ Best practice considerations for retention of personal health information, including records to be retained, length of time for retention and setting up a retention schedule</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #12: Considerations for Retention of Personal Health Information</i></li> <li>▪ IPWG. <i>Fact Sheet #18: Considerations for Destruction and Disposal of Personal Health Information</i></li> <li>▪ IPC. <i>Fact Sheet Number 1: Safeguarding Personal Health Information:</i> <a href="http://www.ipc.on.ca/images/Resources/fact-01-e.pdf">http://www.ipc.on.ca/images/Resources/fact-01-e.pdf</a></li> <li>▪ College of Physicians and Surgeons of Ontario: Policy Number 5-05: Medical Records: <a href="http://www.cpso.on.ca/policies/policies/default.aspx?id=1686">http://www.cpso.on.ca/policies/policies/default.aspx?id=1686</a></li> </ul>
Safeguards	<ul style="list-style-type: none"> <li>▪ Best practice considerations for the access, transfer and transport, mobile devices and media, encryption and third-party agreements</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #13: Safeguarding Personal Health Information</i></li> <li>▪ IPWG. <i>Fact Sheet #14 Mobile Devices and Media and Personal Health Information</i></li> <li>▪ IPWG. <i>Fact Sheet #15: Personal Health Information Transmittal via Fax</i></li> <li>▪ IPWG. <i>Fact Sheet #16: Third-Party Data Sharing Agreements</i></li> <li>▪ IPWG. <i>Fact Sheet #17: E-Mail and Personal Health Information</i></li> <li>▪ IPWG. <i>Fact Sheet #24: Password Strategies and Best Practices</i></li> <li>▪ IPC. <i>Fact Sheet: Safeguarding Personal Health Information:</i> <a href="http://www.ipc.on.ca/images/Resources/fact-01-e.pdf">http://www.ipc.on.ca/images/Resources/fact-01-e.pdf</a></li> <li>▪ IPC. <i>Fact sheet: Health Care Requirement for Strong Encryption:</i> <a href="http://www.ipc.on.ca/images/Resources/fact-16-e.pdf">http://www.ipc.on.ca/images/Resources/fact-16-e.pdf</a></li> <li>▪ IPC. <i>Fact sheet: Wireless Communication Technologies:</i> <a href="http://www.ipc.on.ca/images/Resources/up-1fact_14_e.pdf">http://www.ipc.on.ca/images/Resources/up-1fact_14_e.pdf</a></li> <li>▪ North Bay Parry Sound District Health Unit: <i>Third-Party Access Policy</i></li> <li>▪ Region of Waterloo Public Health. <i>Policy and Procedure Manual: Handling PHI outside of ROWPH premises</i></li> </ul>

Curriculum Topics	Notes	Available Training Resources
		<ul style="list-style-type: none"> <li>▪ Huron County Health Unit. <i>Policies and Procedures: Passwords</i></li> <li>▪ Huron County Health Unit. <i>Policies and Procedures: Mobile Computing Devices and Mobile Media</i></li> <li>▪ Halton Region Health Department. <i>Policy: Providing PHI by E-mail</i></li> <li>▪ USA Department of Health and Human Services. <i>HIPAA security series. Security Standards: Administrative Safeguards:</i> <a href="http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf">http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf</a></li> <li>▪ USA Department of Health and Human Services. <i>HIPAA security series. Security Standards: Physical Safeguards:</i> <a href="http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf">http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf</a></li> <li>▪ USA Department of Health and Human Services. <i>HIPAA security series. Security Standards: Technical Safeguards:</i> <a href="http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf">http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf</a></li> </ul>
Disposal	<ul style="list-style-type: none"> <li>▪ Best practice considerations for the safe disposal and destruction of PHI</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #18: Considerations for Destruction and Disposal of Personal Health Information</i></li> <li>▪ IPC. <i>Secure Destruction of Personal Information :</i> <a href="http://www.ipc.on.ca/images/Resources/fact-10-e.pdf">http://www.ipc.on.ca/images/Resources/fact-10-e.pdf</a></li> <li>▪ York University: <i>Tip sheet #7, Secure Destruction of Records</i></li> </ul>
Managing a privacy incident/breach	<ul style="list-style-type: none"> <li>▪ Awareness of key responsibilities and actions to be taken when an incident is suspected/occurs</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #19: Considerations for Handling A Privacy Incident or Breach</i></li> <li>▪ IPC. <i>What to do if a privacy breach occurs:</i> <a href="http://www.ipc.on.ca/images/Resources/priv-breach-e.pdf">http://www.ipc.on.ca/images/Resources/priv-breach-e.pdf</a></li> <li>▪ Region of Waterloo Public Health. <i>Policy and Procedure Manual: Lost/Stolen PHI and Unauthorized Access</i></li> <li>▪ York Region Community and Health Services Department: <i>Protocol for Managing Privacy Breach</i></li> <li>▪ Durham Region Health Department. <i>Privacy Policy: Appendix A</i></li> <li>▪ Ottawa Public Health Department. <i>PHIPA Breach Procedure</i></li> </ul>
Individual Access	<ul style="list-style-type: none"> <li>▪ Understanding the legislative provisions for access to one's own PHI and best practice considerations</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet # 20: Considerations for Requests for Access to and Correction of Personal Health Information</i></li> <li>▪ IPWG. <i>Fact Sheet #21: Considerations for Responding to Requests for Use, Disclosure or Access to Personal Health Information</i></li> <li>▪ IPC. <i>Fact Sheet #2: Your health information, your access and correction rights:</i> <a href="http://www.ipc.on.ca/images/Resources/fact-02-e.pdf">http://www.ipc.on.ca/images/Resources/fact-02-e.pdf</a></li> <li>▪ IPC. <i>PHIPA Practice Direction: Clarifying Access Requests:</i> <a href="http://www.ipc.on.ca/images/Resources/up-1he_pd_01_e.pdf">http://www.ipc.on.ca/images/Resources/up-1he_pd_01_e.pdf</a></li> </ul>

Curriculum Topics	Notes	Available Training Resources
		<ul style="list-style-type: none"> <li>▪ York Region Community and Health Services Department. <i>Requests for Access to or Correction of Information</i></li> <li>▪ Region of Waterloo Public Health. <i>Policy and Procedure Manual: Access Requests for PHI</i></li> <li>▪ Niagara Region Health Department. <i>Release of Personal Health Information</i></li> </ul>
<p>Accuracy and Complaints Procedures (Challenging Compliance)</p>	<ul style="list-style-type: none"> <li>▪ Understanding the legislation surrounding requests for correction of an individual's PHI and handling complaints</li> </ul>	<ul style="list-style-type: none"> <li>▪ IPWG. <i>Fact Sheet #22: Fair Information Practices – Accuracy and Managing Complaints</i></li> <li>▪ York Region Community and Health Services Department. <i>Dealing with complaints</i></li> <li>▪ Region of Waterloo Public Health. <i>Policy and Procedure Manual: Complaints about the handling of PHI</i></li> </ul>

## ACKNOWLEDGEMENTS

### *Information Privacy Working Group (IPWG)*

The Association of Local Public Health Agencies and the Ministry of Health and Long-Term Care wish to thank the members of the Information Privacy Working Group for their contribution to the development of both the Training Strategy and associated Tool Kit:

*Michèle Harding,*

Manager(A), Public Health Standards,  
Practice and Accountability Branch,  
MOHLTC  
Co-Chair IPWG

*Robert Kyle,*

Commissioner & Medical Officer of Health,  
Durham Region Health Department/alpha  
Co-Chair IPWG

### **Members from Health Units and other Organizations:**

Dr. Eileen deVilla, AMOH, Peel Public Health Unit

Dr. Michael Finkelstein, AMOH, Toronto Public Health

Ms. Pat Hewitt, Manager, Public Health Administration, Halton Region Health Department/  
Performance Management Working Group Representative

Dr. Valerie Jaeger, MOH(A), Niagara Region Public Health Department

Mr. Bill Mindell, Director of Clinical Services, Simcoe Muskoka District Health Unit

Dr. Lynn Noseworthy, MOH, Haliburton, Kawartha, Pine Ridge District Health Unit

Ms. Jane Speakman, City Solicitor, City of Toronto

Ms. Linda Stewart, Executive Director, alpha

Dr. Bryna Warshawsky, AMOH, Middlesex-London Health Unit

### **Provincial Members:**

Ms. Mary Lou Daniels, Privacy Officer, Public Health Ontario (PHO)

Mr. Paul Kaufman, Counsel, Legal Service Branch, MOHLTC/MHPS

Ms. Shelley Laskin, Senior Advisor, Ministry of Health Promotion and Sport (MHPS)

Mr. Andrew Lefebvre, Senior Analyst, Protection and Prevention Branch, Ministry of Health and Long-Term Care (MOHLTC)

### **Secretariat Staff:**

Ms. Candace AQUI, Mr. Doug Gowans and Ms. Nicole Consitt, Standards, Practice & Accountability Branch, MOHLTC

Mr. Shawn Hewitt and Ms. Jennifer Dempster, Knowledge Management Branch, MOHLTC