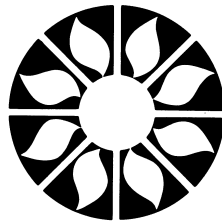


**Simplifying Privacy:
a Tool Kit for
Long-Term-Care and
Community Care**

(This is OANHSS's disclaimer page – other association will want to add there own here)

Simplifying Privacy
A Tool Kit for Long-Term Care Facilities and Community Care
Published by



OANHSS

Ontario Association of Non-Profit Homes and Services for Seniors
7050 Weston Road, Suite 700, Woodbridge, Ontario L4L 8G7

Phone (905) 851-8821 • Fax (905) 851-0744

Simplifying Privacy a Tool Kit for Long-Term Care Facilities and Community Care is distributed for information purposes only, with the understanding that the Ontario Association of Non-Profit Homes and Services for Seniors (OANHSS) is not engaged in rendering legal or other professional advice.

If legal advice or other expert assistance is required, the services of a professional should be sought. In addition, the opinions expressed by the contributors to this work are their own and do not necessarily reflect the opinions or policies of OANHSS.

OANHSS represents and supports the common goals of its members to provide and advocate for quality housing and long-term care programs and services.

ISBN 0-921092-62-8

Acknowledgements *OANHSS had a number of members review this material – the members represented all sectors except CCACs) They are acknowledged here)*

The production of this publication would not have been possible without the valuable information and insights provided by OANHSS facility members, the government and legal experts and the consultants who researched and prepared the content. These contributors have played a vital role by generously contributing their expertise, energy and time. OANHSS wishes to extend its thanks and appreciation to the following members:

- Carolyn Vandermolten.....Saint Luke’s Place
- Dan DelisleI.O.O.F. Senior Citizen Homes Inc
- Debbie Fujina.....Momiji Health Care Society
- Janet MorrisPerley and Rideau Veterans’ Health Centre
- John Buma.....Albright Centre
- Norm CreenBelmont House
- Oris Retallack.....Unitarian House
- Reg Crawford.....Belvedere Heights

Special thanks are extended to Heather Black, Assistant Commissioner, Privacy Commissioner of Canada, Brendan Seaton, Chief Privacy & Security Officer, Smart Systems for Health Agency, SMART Systems for Health and Patrick Hawkins, a lawyer with Borden Ladner, Gervais, LL.P.

The consultants who developed the publication are:

Jeanne Bickle, BScN
Bickle Associates Inc.
Tel: 905 857 9493
Jbickle@sympatico.ca

Lois Cormack, MHSc, CHE
Tel: 416-802-8096
Lois.cormack@sympatico.ca

Limitations for Users of the Tool Kit

The Tool Kit is designed to assist long-term-care and community care organizations in reviewing their own privacy policies and practices. It is important that each organization conducts a review of how personal information and personal health information are collected, used and disclosed within their organizations, and then to consider whether their policies and practices need to be modified to bring them into agreement with current privacy principles. The Tool Kit is not meant to replace that review. The templates are generic templates only. The organization should carefully consider whether or not the particular template is appropriate for use within their organization and modify it as appropriate.

This publication was supported by the Ontario Ministry of Health and Long-Term-Care (MOHLTC) and prepared on behalf of Continuing Care e-Health Council.

Document Map

This Tool Kit is divided into 4 sections for easy reference.

Section 1 – Privacy Explained

- ?? Background on Privacy
- ?? Guidelines and the CSA Code
- ?? Privacy legislation
- ?? Privacy program requirements

Section 2 – Implementation Phases

- ?? Project structure
- ?? Privacy reviews
- ?? Implementation steps
- ?? Sustaining gains achieved

Section 3 – Implementation Tools

- ?? Templates (WORD)
- ?? Work plan (EXCEL)
- ?? Educational Presentations (PowerPoint)
- ?? Communication

Section 4 – Frequently Asked Questions

- ?? Generic
- ?? Specific to Long-term-care and Community Care

Please refer to the Table Of Contents following for a complete listing of subject headings and page numbers.

Table of Contents

Section 1 — Privacy Explained

1.	Introduction.....	9
2.	About Privacy	10
3.	Privacy Guidelines and the CSA Code	11
4.	Privacy Legislation.....	14

Section 2 — Implementation Phases

<i>Phase I</i> –	6.1	<i>Project Structure</i>	18
		a. Privacy Officer and Privacy Office Function	19
		b. Organizational Privacy Governance.....	19
		d. Work Plan.....	20
		e. Privacy Steering Committee	20
		f. Communications	20
<i>Phase II</i> –	6.2	<i>Privacy Review</i>	20
		a. Conduct a Privacy Review and Gap Analysis	22
		b. Privacy Impact Assessment (PIA)	23
		c. Privacy Plan	24
		d. Organization-Wide Privacy Policy	24
<i>Phase III</i> –	6.3	<i>Implementation</i>	26
		a. The Notice Form	26
		b. Consent.....	27
		c. Safeguards.....	32
		d. Need-To-Know.....	32
		e. Employee Information	34
		f. Staff Education	34
		g. Third Party Contracts	35
		h. Confidentiality Provisions for Supplier Agreements	36
<i>Phase IV</i> –	6.4	<i>Sustaining the Gains</i>	37
		a. Privacy Officer / Office	37
		b. Privacy Check List.....	37
		c. Communications	37
		d. Handling Complaints.....	38
		e. Privacy Policies	38

Section 3 — Implementation Tools (Refer to section numbers above)

<i>Phase I</i> –		<i>Project Structure</i>	
	6.1 a.	Template: Job Description of a Privacy Officer.....	40
	6.1 b.	Template: Privacy Office Functions.....	41
	6.1 c.	Spreadsheet: Work Plan (picture).....	42
	6.1 d.	Template: Steering Committee Terms of Reference.....	43
	6.1 e.	Template: Sample Communications Bulletin	44

continued ...

... Table of Contents continued

Phase II –	Privacy Review	
6.2 a.	Template: Privacy Review Questionnaire	45
6.2 b.	Template: Gap Analysis	47
6.2 c.	Template: Privacy Impact Assessment	48
6.2 d.	Template: Risk and Mitigation Strategies	50
6.2 e.	Template: Privacy Plan	52
6.2 f.	Template: Organization-Wide Privacy Policies	53
Phase III –	Implementation	
6.3 a.	Template: Notice Form	57
6.3 b.	Template: Consent Form	62
6.3 c.	Template: Letter for Fundraising Lists	64
6.3 d.	Template: Employee Confidentiality Policy and Agreement.....	65
6.3 e.	Template: Safeguard Policies	67
6.3 f.	Presentation: Staff Education (PowerPoint presentations)	69
6.3 g.	Template: Third Party Contract	70
6.3 h.	Template: Confidentiality Provisions for Supplier Agreements.....	72
Phase IV –	Sustaining the Gains	
6.4 a.	Template: Privacy Check List.....	76
6.4 b.	Template: Handling Complaints	79
6.4 c.	Brochure: Sample Brochure.....	80

Section 4 — Frequently Asked Questions and Bibliography

7 a.	Generic Privacy FAQs	85
7 b.	FAQs specific to Long-term-care and Community Care	88
7 c.	FAQs for not-for-profit organizations.....	95
8.	Bibliography.....	99

Section 1 – Privacy Explained

1.	Introduction	9
2.	About Privacy.....	10
3.	Privacy Guidelines and the CSA Code.....	11
4.	Privacy Legislation	14

1. Introduction

Purpose: This Privacy Tool Kit will:

1. Explain good information management practices as defined within the meaning of Privacy Principles, and
2. Provide ready-to-use tools for those who must implement Privacy practices in long-term-care and community care organizations.

Although most users of this tool kit will have competing priorities and concerns that are operational, it will be helpful to remember that the big Privacy picture is global in scope. Short-term and stand-alone projects undertaken with the help of this tool kit should be viewed as part of a broader ongoing process.

Privacy requirements are driven by privacy principles and legislation. The tool kit is structured along 4 phases of implementation designed to both enable organizations to understand current privacy principles and to implement a privacy program consistent with these principles. It is suggested that the 4 phases be followed in sequence at a pace that is in keeping with resources and other organizational commitments. It is recommended, however, that long-term-care and community care will have started to look at privacy in their organizations by January 1, 2004, using the tools provided herein. It is reasonable to expect that implementation will continue for 6 months to 1 year depending on the size and complexity of the organization.

Designating an individual to be responsible for Privacy is the recommended first step, followed immediately by a workable plan and timetable. The plan should cover, as a minimum, policies and procedures for both individual access and handling complaints, developing a Notice and Consent form (which also includes consent for fundraising purposes), and staff training on privacy principles.

2. About Privacy

Why is **Privacy** important? Privacy is fundamental to a free and democratic society. Freedoms of speech and religion, or simply to be let alone, are all based on the basic right of individuals to their privacy.

What is covered by the term "**Personal Information**"? Personal Information is "information about an identifiable individual" that includes any personal information, recorded or not, in any form, including digital or paper format. *Personal information of a sensitive nature*, may include health or medical history, racial or ethnic origin, political opinions, religious beliefs, trade union membership and sexual orientation.

There are three fundamentals to bear in mind when considering the privacy of personal information strictly from the viewpoint of the individual:

1. The individual described by the personal information controls it – not the organization holding the information.
2. Privacy is not about preventing access to an individual's information. It is about allowing information to be collected, used and disclosed in accordance with the specific wishes of the individual.
3. Privacy, Security and Confidentiality are not the same thing. Although there is some overlap in definition, their individual meaning and intent must not be confused.
 - ?? **Privacy** relates to people, process and accountability. It gives individuals control over their personal information, and requires them to grant permission to an organization for the collection, use, disclosure and retention of that information.
 - ?? **Security** is the essential component for preventing inadvertent release of personal information. Security also relates to the availability and integrity of personal information.
 - ?? **Confidentiality** addresses only the disclosure of personal information.

There is a similar set of fundamentals pertaining to organizations. In recent years we have seen unparalleled growth in the ability of organizations to collect, compile, analyze and disseminate personal information. In fact, there is already a significant volume of health related personal information currently available in electronic form.

Failure to meet client expectations regarding privacy, or breaking faith with them through misuse of their personal information, can easily attract negative media coverage and potentially expose the organization to legal liabilities, fees and damage.

3. Privacy Guidelines and the CSA Code

Privacy Principles: 10 internationally accepted principles lie at the core of organizational responsibilities for safeguarding personal information. These are the global standard for privacy protection, having been defined originally in the 1960s by the Organization for Economic Cooperation and Development (OECD). In Canada the Canadian Standards Association incorporated them into our own set of principles in 1996, now known as the CSA Model Code for the Protection of Personal Information, **the CSA Code**.

For the purpose of the tool kit the 10 CSA Code descriptions that follow have been grouped and categorized under 2 headings: **Principles of Substance** (what needs to be done), and **Principles of Procedure** (how to do it).

Principles of Substance (4):

Principles of substance specify what organizations must do in order to comply with the CSA Code. For example, the purposes for collecting information must be provided to the individual or the substitute decision maker, and their consent must be obtained after the purposes have been explained. The amount of information collected from the individual or the SDM is limited to the purposes identified, and it may only be used, disclosed or retained for that purpose.

Principle 2 - Identifying Purpose

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

Principle 3 - Consent

The knowledge and consent of the individual is required for the collection, use or disclosure of personal information. It is understood that obtaining consent may be inappropriate or impossible when the individual is a minor, seriously ill, or mentally incapacitated. In such cases consent must be obtained from the substitute decision maker (SDM).

Principle 4 - 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.

Principle 5 - 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.

Principles of Procedure (6):

Principles of Procedure tell organizations how to apply the principles of substance listed above. Organizations are accountable for the personal information under their control, and they must ensure that it is accurate and kept safe. They must also be open about their information management practices, allowing individuals to access their personal information and amend it if it is not accurate. Individuals must be able to complain if he or she is concerned that an organization has not complied with privacy requirements.

Principle 1 - 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 privacy principles

Principle 6 - 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.

Principle 7 - Safeguards

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

Principle 8 - Openness

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

Principle 9 - 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.

Principle 10 - 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.

In summary, the primary focus of the 10 privacy principles described above is on obligations that must be borne by the service organization. Users of the Tool Kit might also find it helpful to re-read them from the viewpoint of the individual.

?? **Control** - The individual has the right to provide or withhold consent

?? **Knowledge** - The individual must have knowledge about how his or her personal information will be used or disclosed. An organization cannot use or disclose an individual's personal information unless the individual is informed as to how the personal information will be used or disclosed.

- ?? **Access** - The individual must be given access to his or her personal information upon request and must have the ability to amend personal information if it is not correct.
- ?? **Recourse** - The individual has a right to complain if his or her information is compromised.

4. Privacy Legislation

The fundamental issue of Privacy has always been supported by appropriate government legislation, beginning with 'data protection' laws enacted in Europe during the 1960s and 1970s. Canada's entry began with the Canada Privacy Act in 1982. Current information from Europe and the U.S. is readily available for those who need a global perspective on Privacy legislation.¹

For the purposes of this tool kit we will limit these discussion specific pieces of Canadian legislation. Although we must remain cognizant of wider information networks in our modern electronic age, these will serve to cover immediate operational concerns.

PIPEDA — The Personal Information Protection and Electronic Document Act comes into effect on January 1, 2004 and will apply to organizations in Canada that collect, use or disclose personal information in the course of "commercial activities". It is part of a global trend covering personal data protection and is based on privacy principles that are internationally accepted. These are the same principles described in the CSA Code, defining the core values for privacy in Canada.

When PIPEDA was first introduced in January 2001 it applied only to federally regulated organizations. It is not totally clear at this time to what extent the Act will apply to all of the activities of long-term-care facilities and community care organizations in Ontario because of the "commercial activities" definition. However, fund-raising activities fall into this category and therefore will be subject to PIPEDA.

The privacy principles defined in PIPEDA reflect current privacy thinking. They provide a good model for policy development and information management practices. It is reasonable to expect that any new provincial privacy legislation will be similar to the federal law. Steps taken now to comply with the federal legislation will not be wasted and will take long-term-care and community care organizations a long way towards complying with any new provincial legislation. Furthermore, the public will begin to expect long-term-care and community care organizations to adhere to these privacy principles.

FIPPA — The Ontario Freedom of Information and Protection of Privacy Act applies to Ontario's provincial ministries and agencies, boards and most commissions, as well as community colleges and district health councils. This Act requires that the government protect the privacy of an individual's personal information existing in government records. It also gives individuals the right to request access to government information, including most general records and records containing their own personal information.

MFIPPA — The Ontario Municipal Freedom of Information and Protection of Privacy Act applies to municipalities, local boards, agencies and commissions. This may include information held by a city clerk, a school board, board of health, public utility, police commission or municipal and district homes for the aged and housing and community services. It requires that local government organizations protect the privacy of an

¹ Links to international privacy sites: http://www.privcom.gc.ca/information/links-liens_e.asp

individual's personal information existing in government records. It also gives individuals the right to request access to municipal government information, including most general records and records containing their own personal information.

FIPPA and MFIPPA — Both includes rules regarding the collection, retention, use, disclosure and disposal of personal information in the organization's custody or control. If an individual feels his or her privacy has been compromised by a government organization governed by the Act, he or she may complain to the Information and Privacy Commissioner for Ontario who may investigate the complaint. Individuals who are given access to their personal information have the right to request correction of that information where they believe there may be an error or omission. Where this request is refused, individuals may require that a statement of disagreement be attached to the information. Individuals may also require that all parties to whom the information has been disclosed in the preceding year be notified of the correction or statement of disagreement.

PIPEDA and MFIPPA — According to the Privacy Commissioner of Canada, municipal and district homes, housing and community services are subject to MFIPPA, and are therefore not subject to PIPEDA. If the MFIPPA organization is engaged in commercial activity outside its mandate, it can be argued that such activity is within its mandate and not covered by PIPEDA. If an organization is covered by MFIPPA and the information collected, used or disclosed in the course of the activity is subject to the provisions of MFIPPA then there is a prima facie argument that the activity is within the mandate of the organization and therefore not an activity covered by PIPEDA.

If the Office of the Privacy Commissioner of Canada is compelled to take jurisdiction over an MFIPPA organization, the Office can say, under S. 13(2), that the complaint is best dealt with under provincial law and decline to issue a report. The Office of the Privacy Commissioner of Canada does not want to be involved where there is provincial recourse, e.g. to the Office of the Privacy Commissioner for Ontario.²

Other Ontario Legislation

Draft provincial privacy legislation - Draft privacy legislation was circulated for consultation purposes in 2002. Although it was clear that the health community supported the introduction of such legislation, it was not introduced. Consequently, health care organizations, starting January 1 2004, will be subject to PIPEDA. There is currently no assurance that Ontario will introduce privacy legislation for the health sector.

The Health Care Consent Act — This Act outlines rules for consent with respect to treatment. Even though the same rules may be applied to consent for the collection, use, disclosure and retention of personal information, the two must be treated as separate issues. They each have separate and distinct forms and they may not be combined.

The Substitute Decisions Act — This Act puts on record the names of specific people who can make decisions on behalf of an individual. The rules outlined in the Substitute

² Memo to OANHSS, November 6, 2003, from the Assistant Commissioner, the Office of the Privacy Commissioner for Canada

Decisions Act may be followed when obtaining consent for the collection, use, disclosure and retention of personal information.

Ontario's Regulated Health Professions Act - The Regulated Health Professions Act defines the statutory obligations of regulated health professionals to protecting personal health information. This legislation and common law has requirements about confidentiality and access to resident and client health data.

In addition:

The following Acts should be considered in the context of Privacy.

- ?? The Long term Care Act
- ?? The Nursing Home Act
- ?? Homes for Aged and Rest Homes Act
- ?? Charitable Institutions Act
- ?? Tenant Protection Act

The chart below provides an overview of legislative comparisons in relation to the Privacy Principles.³

Legend: Y = Yes
 N = No
 P = Partially

Principle	PIPEDA	MFIPPA	LTC Act	Nursing Home Act	Homes for the Aged & Rest Home Act	Charitable Institutions Act	Tenant Protection Act
Accountability	Y	Y	N	N	N	N	N
Defined Purposes	Y	P	N	N	N	N	N
Consent	Y	Y	Y	N	N	N	N
Limiting Collection	Y	P	N	N	N	N	N
Limiting Use Disclosure Retention	Y	P	Y	Y	N	N	N
Accuracy	Y	P	N	P	N	N	N
Safeguards	Y	N	N	N	N	N	N
Openness	Y	Y	Y	N	N	N	N
Individual Access	Y	Y	Y	N	N	N	N
Challenging Compliance	Y	Y	P	N	N	N	N

³ "Privacy Compliance for the Not-for-Profit Sector Slide Presentation, by Brendan Seaton, Chief Privacy and Security Officer, Smart Systems for Health Agency, OANHSS Privacy Compliance Conference, October 30 2003"

Section 2 – Implementation Phases

Phase I – 6.1	Project Structure	18
	a. Privacy Officer and Privacy Office Function	19
	b. Organizational Privacy Governance	19
	d. Work Plan	20
	e. Privacy Steering Committee.....	20
	f. Communications	20
Phase II – 6.2	Privacy Review	20
	a. Conduct a Privacy Review and Gap Analysis.....	22
	b. Privacy Impact Assessment (PIA)	23
	c. Privacy Plan.....	24
	d. Organization-Wide Privacy Policy.....	24
Phase III – 6.3	Implementation	26
	a. The Notice Form.....	26
	b. Consent	27
	c. Safeguards	32
	d. Need-To-Know	32
	e. Employee Information	34
	f. Staff Education	34
	g. Third Party Contracts	35
	h. Confidentiality Provisions for Supplier Agreements.....	36
Phase IV – 6.4	Sustaining the Gains	37
	a. Privacy Officer / Office.....	37
	b. Privacy Check List.....	37
	c. Communications.....	37
	d. Handling Complaints	38
	e. Privacy Policies	38

Privacy Program Implementation

The process of meeting the new Privacy requirements presents an opportunity for organizations to review processes, address risks and streamline forms and procedures. Following is a proposed approach with four separate phases to assist organizations with implementation.

Phase I	Putting a project structure in place	4 weeks
Phase II	Conducting A Privacy Review and Developing a Privacy Plan	4-6 months
Phase III	Implementing the Plan	4- 6 months
Phase IV	Sustaining the Gains	Ongoing

6.1 Phase I – The Project Structure (4 weeks)

To prepare the organization to undertake the privacy project, clear roles and responsibilities should be assigned and a work plan developed. A potential structure would include:

- A. Privacy Officer and Privacy Office Function
- B. Organization Privacy Governance
- C. A Privacy Project Work Plan
- D. A Privacy Steering Committee
- E. Communications

a. Privacy Officer and Privacy Office Function

Principle one of the CSA Code states “an individual or individuals shall be designated who are accountable for the organization’s compliance with privacy principles”. Each organization is therefore required to appoint an individual to be responsible for the privacy practices of the organization. The function of a Privacy office should be established to be accountable for privacy practices on an ongoing basis and be managed by the privacy officer to ensure continuous improvement of the privacy program. It may be beneficial to assign responsibility for the privacy office function at the beginning of the privacy project, which can be maintained after the plan is implemented.

Functions of the privacy office include:

- ?? addressing privacy questions, concerns and challenges to the organization and third parties
- ?? ensuring continuous improvement of information management practices
- ?? ongoing privacy training for all staff
- ?? updating and revision of privacy policies
- ?? provide and track access for individuals to their personal information

- ?? implement and maintain a dispute mechanism
- ?? perform audits on data repositories, systems and processes
- ?? manage events (e.g. breaches of privacy)

It will be helpful if the individual appointed to Privacy Officer holds a senior leadership position in the organization and has the authority to implement a privacy program, access resources and address issues that do not meet organizational expectations.

In long-term-care and community care organizations it is most likely that the role of the privacy officer, along with the responsibilities of the privacy office, will be assigned to an existing position as additional responsibilities.

TOOL: Refer to Section 3, Template 6.1a, for a suggested Privacy Officer’s Job Description. This can also be viewed as a ready-to-use WORD document at {[hyperlink](#)}.

TOOL: Refer to Section 3, Template 6.1b, for an outline of Privacy Office functions. This can also be viewed as a ready-to-use WORD document at {[hyperlink](#)}.

c. Organizational Privacy Governance

As part of the overall organizational structure of the company, a privacy governance structure will need to be established to manage privacy. This structure will be responsible for approving privacy policies, addressing privacy issues that affect the organization as a whole, and for ensuring that the organization and third parties, practice according to the organization’s privacy policies and practices.

This may involve defining terms of reference for a new committee or adding to the terms of reference of an existing management team or board committee.

Responsibilities include:

- ?? Having an understanding of the 10 Privacy Principles.
- ?? Understanding the benefits of having a Privacy Program in place
- ?? Approving organizational privacy policies
- ?? Making decisions on privacy issues that affect the organization and allocating resources as required
- ?? Ensuring that the organization and third parties comply with the organization’s privacy policies and practices
- ?? Monitoring the progress of the privacy project and ensuring leaders in the organization are supportive of the process

The committee responsible for organizational privacy governance could manage the privacy project or a separate privacy Steering Committee could be established to direct the implementation of a privacy program, depending on the size and complexity of the organization.

d. Work Plan

The individual appointed as Privacy Officer should develop a work plan and educational materials for presentation and discussion at the first privacy steering committee meeting. The work plan should include all project phases and timelines, including the roles and responsibilities of staff involved in the plan.

TOOL: Refer to Section 3, illustration 6.1c, for a spreadsheet outlining a draft work plan. This can also be viewed as a ready-to-use Excel work sheet at {hyperlink}.

e. Privacy Steering Committee

The privacy Steering Committee should be representative of key positions in the organizations, be chaired by the Privacy Officer and oversee the privacy review and privacy plan implementation.

The work of the privacy steering committee could become part of an existing committee or part of the management team's responsibilities and terms of reference.

The steering committee develops communications and may assist with staff education. Individuals selected for the privacy steering committee should be formal or informal leaders, keen to learn about privacy and develop expertise in the area, knowledgeable about the organizations information management practices and possess good communications skills. The privacy steering committee members will need to be available for the meetings and be willing to commit some time to learning and contributing to a new body of knowledge in the organization.

The first meeting of the privacy steering committee may include the following:

- ?? Provide a privacy overview (Privacy and the 10 Principles presentation 6.3f)
- ?? Review the project plan
- ?? Review the compliance questionnaire
- ?? Assign members to working groups
- ?? Develop communications plan

TOOL: Refer to Section 3, Template 6.1d, for the Steering Committee's Terms of Reference. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

f. Communication

Implementation of an organization-wide privacy program will provide the organization with the opportunity to promote its commitment to protecting the integrity and privacy of personal information about its clients. A communications package, providing information about the privacy project, will need to be developed and shared with residents, families,

staff, volunteers, all stakeholders and with the community at large. The communications methods and timing should be discussed and planned for by the privacy steering committee at each meeting and included in the work plan.

Ongoing communications content may include results of the privacy review, the privacy plan and implementation progress. Communications methods could include frequently asked questions (FAQs) or case scenarios, communicated using the usual means including attachment to pay stubs and on staff bulletin boards.

TOOL: Refer to Section 3, 6.1e, for a sample Communications Bulletin. This template can also be opened as a ready-to-use WORD document at {[hyperlink](#)}.

6.2 Phase II – The Privacy Review (4-6 months)

Phase II includes:

- A. Conducting a Privacy Review and Gap Analysis
- B. Conducting a Privacy Impact Assessment
- C. Developing a Privacy Plan
- D. Developing Organizational Privacy Policies

a. Conduct a Privacy Review

Conducting a privacy review enables an organization to assess how they are currently managing privacy across the organization. The privacy review focuses the attention of senior management on what needs to be done throughout the organization and the risks of non-compliance. The initial review will involve the completion of compliance questionnaires for each department or the organization as a whole. For multi-facility organizations/offices it may be useful to conduct an organization-wide privacy review prior to individual facility/office reviews. The questionnaire(s) will:

- ?? Identify existing policies and procedures to be revised or need for new ones
- ?? Determine the extent of staff education required
- ?? Track the flows of personal information within the organization and externally
- ?? Catalogue all data repositories, information systems, data processes and forms that collect, use, disclose or retain personal information
- ?? Identify the need for privacy impact assessments (PIAs)*
- ?? Assess how personal information is collected, used and disclosed
- ?? Determine the deficiencies (regarding adherence to privacy practices) in third party contracts

The privacy steering committee should review the questionnaire provided and customize it for the organization.

Each area in the organization should complete a questionnaire over a given period of time and all of the results should be compiled for analysis by the privacy steering committee.

Note: The Privacy Review is a lengthy process. Ensure that the appropriate time is allotted to the review activity. Complete the privacy review in a timeframe that is manageable in your organization.

Complete a Gap Assessment

Once the privacy review is completed, the organization will be able to identify gaps in how it collects, uses and discloses personal information. These gaps must be assessed and a determination made about the level of risk these gaps impose on the organization. The steering committee will define the risks associated with the gaps and determine the

mitigation strategies that need to be implemented to ensure the organization has information practices that are consistent with the 10 privacy principles. A Privacy Plan is created that outlines the actions to be taken to effectively mitigate privacy risks.

Based on the results of the privacy review questions and the gap analysis, each area should develop a plan to ensure privacy issues are managed in a manner consistent with the organization's plan.

TOOL: Refer to Section 3, Templates 6.2b and 6.2 d, for Templates showing a Gap Analysis. These can also be viewed as a ready-to-use WORD documents at [{hyperlink}](#).

b. Privacy Impact Assessment (PIA)

A PIA is a process or methodology used to determine whether information systems and technologies will meet or are meeting the privacy requirements of the CSA Code and privacy legislation.

The PIA is designed to ensure that privacy is considered throughout all aspects (transactions – collections, use, disclosures and retention).

It is recommended that a PIA be completed when:

- ?? An information system contains a large amount of sensitive personal information and is used frequently by many/most staff, e.g. the clinical information system.
- ?? When a new data repository is created, e.g. the implementation of an electronic clinical information system.
- ?? When an existing system is modified significantly.
- ?? When information systems are linked, e.g. financial with clinical.
- ?? Wherever there may be privacy risks, e.g. personal information is transmitted using the internet.

The goals of the PIA are to:

- ?? Enable management to make informed decisions about information systems based on an understanding of the risks, e.g. do they need to be replaced, or upgraded with more access controls and expanded logging and tracking capability.
- ?? Ensures that accountability for privacy issues in systems is clearly incorporated into the responsibilities of information system developers and managers.
- ?? Ensures a consistent format and structured process for analyzing both organizational and technical compliance with privacy principles.
- ?? Ensures that protection for privacy is included in the development or modification and enhancements of information technology projects.
- ?? Provides basic documentation on the flow of personal information.

The Benefits of doing a PIA on information systems include:

- ?? Facilitates consistency with privacy legislation and the CSA Code.
- ?? Promotes awareness and understanding of privacy issues.
- ?? May eliminate the need for costly programs and/or system re-engineering.

TOOL: Refer to Section 3, Template 6.2 c, for Instructions and Templates on Privacy Impact Assessment. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

c. Privacy Plan

The privacy plan summarizes the findings of the privacy review, documents the gaps, risks and defines the actions to mitigate the risks that will improve information management practices through out the organization, consistent with privacy principles. Developing the organization's privacy plan is the single largest component of the project. The plan should include actions, dates, accountabilities and required resources. The organizational governance team should approve the privacy plan prior to beginning implementation.

TOOL: Refer to Section 3, Template 6.2 e for Instructions and Templates on a Privacy Plan. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

d. Organization-Wide Privacy Policies

The development and enactment of organization-wide privacy policies enables an organization to make a declaration of its beliefs regarding personal privacy and the value placed on it. Organization-wide privacy policies can be used to communicate to clients that their personal information will be respected and honored throughout the organization. The policies inform staff, third parties and stakeholders about the organization's privacy expectations. They also establish a working environment that has a clear commitment to privacy requirements.

The privacy policy provided in Template 6.2 d offers organizations an example of a privacy policy. The policy provided mirrors the privacy policy articulated by the Canadian Standards Association, <http://www.csa.ca/standards/privacy/>

Some organizations may want to modify the CSA privacy policy with language that relates specifically to the services of that organization. This is acceptable, however caution is advised against deleting principles or changing the intent of the principles. The intent of the policies defined in the CSA Code should not be compromised.

It is suggested that organization-wide privacy policies be developed and approved by the steering committee prior to implementation of the privacy program and used as internal working guidelines throughout the implementation phase. Once the privacy program is implemented and the organization has assurances that the privacy policies are being adhered to through out the organization, organization-wide privacy policies can be published.

Note: Once your organization has posted its privacy policy, you may be legally liable if you fail to abide by your privacy policy statements. Only publish your privacy policy when you can confirm that your organization is adhering to the privacy principles you have declared.

It is recommended that legal counsel review the organization-wide privacy policy before it is published.

TOOL: Refer to Section 3, Template 6.2 f, for a Template showing Organization-Wide Privacy Policies. This can also be viewed as a ready-to-use WORD document at [{hyperlink}](#).

6.3 Phase III – Implementation (4 to 6 Months)

The privacy steering committee and privacy officer will oversee implementation of each of the components of the privacy compliance plan and work plan, which may take several months to complete.

- A. Notice Form
- B. Consent (including for fund-raising)
- C. Safeguards
- D. Need to Know
- E. Employee Confidentiality Policy and Agreement
- F. Staff Education
- G. Third Party Contracts
- H. Confidentiality Provisions for Supplier Agreements

a. The Notice Form

Individuals (residents/clients/SDMs) have a right to know how their personal information is to be collected, used, disclosed and stored. This Notice Form identifies the information to be collected by the organization, the purpose for the collection, and the individual's (SDM's) rights under the CSA Code and PIPEDA. It is essential that the Notice become part of the Consent process. The contents of the Notice form must be read by the individual (or SDM) when consent is obtained.

The Notice should include the organization's logo and be posted throughout the organization in public places.

TOOL: Refer to Section 3, Template 6.3a, for a Notice Form. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

Fundraising

Fund raising is an important activity in many long-term-care and community care settings. Under PIPEDA, consent is required for foundation activities. The definition of commercial activity includes: "selling, bartering, or leasing of donor, membership or other fundraising lists", for the purpose of raising money. Grand fathering of old lists is not permitted. In order to use the current mailing lists for fund raising, consent must be obtained.

To address this issue, it is suggested that organizations send a letter to individuals on the fund raising list in the first quarter of 2004.

Note: It is essential that individuals opting out be removed from fundraising lists.

Once the existing fundraising lists have been addressed with the letter, it is suggested that the Notice include fund raising activities. Placing fund raising activities on the Notice

ensures openness and transparency of this important use of personal information. If your organization will not use personal information for fund raising, it is important that the reference to it be deleted from the Notice. Remember that residents, clients or SDMs can refuse to consent to the use of personal information for fund raising activities or can withdraw consent, if previously given. Organizations must have the capability to ensure that residents, clients or SDMs do not receive solicitation for fund raising activities if the consent has been refused or withdrawn.

TOOL: Refer to Section 3, Template 6.3 c, for a suggested letter for fundraising lists. This can also be viewed as a ready-to-use WORD document at [{hyperlink}](#).

Research

Consent is not required for research purposes if the personal information is anonymous; it cannot be linked to an individual and all unique identifiers are removed and information is aggregated. For research that involves the sharing of personal information that can be linked to an individual, express consent must be obtained.

b. Consent

Consent Requirements

The cornerstone of privacy legislation is that the person described by the personal information must be able to control it. The individual named must provide consent for collection, use and disclosure of his/her personal information⁴.

Principle 3 of the CSA Code states “The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.”⁵ (Exceptions to the consent requirement are identified on pages 27 and 28)

In order to consent to the collection, use, and disclosure of personal information, consent must be informed. In the care giving and health care environment, this can be a challenge. It is difficult to determine the balance between enough information (to be knowledgeable) and too much information (to be comprehended). The Notice provided above in section 6.3 An attempts to provide sufficient information for the client to have knowledge.

PIPEDA requires that “express” consent should be obtained for sensitive information. Personal information collected by long-term-care and community care organizations such as: physical or mental health, health services provided, psycho social and financial information would be considered sensitive.

Note: In the Notice Form under “Your rights under the law and the code” it states that “Your information is private. Unless sharing it with others is authorized by law, we cannot and will not give out any of your information without your consent.” It is important to know that PIPEDA allows disclosure of personal information in emergencies, life threatening situations, police investigations, etc.

Types of Consent

Three types of consent are identified: express, implied and notice.

Express consent involves expressly asking the individual for consent to collect, use or disclose the information. Do you consent? The response can be verbal, a simple yes or no. Ideally express consent should be written, e.g. the individual signs a consent form. When verbal consent is used it is recommended that a tick-off box (yes/no) be checked to record that consent was requested.

⁴ The definition of ‘individual’ includes resident, client, tenant, substitute decision maker, spouse, etc.

⁵ ‘Inappropriate’ could be in the event an emergency, life threatening situation, etc. - see PIPEDA Section 7(2) & (3)

A check-off box can be used to enable consent. Individuals can “opt-in” (say yes) or “opt-out” (say no) of information collection activities, e.g. the fundraising mailing list.

Implied consent can occur by specific actions, such as when an individual presents to a laboratory with a requisition for blood work and has blood drawn. Individuals are informed about the collection, uses and disclosures of personal information in a notice form and through discussion with the health professional but are not required to expressly consent to same. They can however, opt out of certain collections, uses, or disclosures as long as the opt out request does not restrict the organization’s ability to process the service application.

Notice is where individuals are given information that is written explaining how their personal information may be used and disclosed but are not asked to sign a form nor are they given a right to opt-out.

Notice, on its own, should not be used in lieu of consent for the application for service process because PIPEDA requires the use of express consent when the information is considered sensitive. A notice form can be reasonably and practicably used in conjunction with the consent process to enable an informed consent. The consent process should identify what information is collected, why it is collected, and the individual’s rights.

The notice form provides this information and is included in section 6.3 a.

Withdrawal of Consent

There are provisions in principle 3 of the CSA Code for the individual to withdraw consent. However, this provision is dependent on whether the withdrawal may impede the provision of services. The organization’s ability to respond to a request for withdrawal of consent must be viewed in the context of the organization’s ability to continue to provide services. If services can not be provided if the consent is withdrawn, the individual cannot withdraw consent.

When is consent obtained?

It is suggested that consent be obtained as part of the application for service process, annually there after (if the individual is still receiving care or services) and when there is a change in purpose, use or disclosure of the information collected.

Other Legislation and Consent

The *Substitute Decisions Act* identifies the specific people who can make decisions on behalf of an individual. The rules outlined in the Substitute Decisions Act should be followed when obtaining consent for the collection, use, disclosure and retention of personal information

The Health Care Consent Act outlines rules for consent with respect to consent for treatment. These same rules may be applied to the consent for the collection, use, disclosure and retention of personal information.

Exceptions to Consent ⁶

Organizations may **COLLECT** personal information without the individual's knowledge or consent only:

- ?? If it is clearly in the individual's interest and consent is not available in a timely manner
- ?? If knowledge and consent would compromise the availability or accuracy of the information and collection is required to investigate a breach of an agreement or contravention of a federal or provincial law
- ?? For journalistic, artistic or literary purposes
- ?? If it is publicly available as specified in the regulations

Organizations may **USE** personal information without the individual's knowledge or consent only:

- ?? If the organization has reasonable grounds to believe the information would be useful when investigating a contravention of a federal, provincial or foreign law **and** the information is used for that investigation
- ?? For an emergency that threatens an individual's life, health or security
- ?? For statistical or scholarly study or research (the organization must notify the Privacy Commissioner of Canada before using this information)
- ?? If it is publicly available as specified in the regulations
- ?? If the use is clearly in the individual's interest and consent is not available in a timely manner
- ?? If knowledge and consent would compromise the availability or accuracy of the information **and** collection was required to investigate a breach of an agreement or contravention of a federal or provincial law.

Organizations may **DISCLOSE** personal information without the individual's knowledge or consent only:

- ?? To a lawyer representing the organization
- ?? To collect a debt the individual owes to the organization
- ?? To comply with a subpoena, a warrant or order made by a court or other body with appropriate jurisdiction
- ?? To a government institution that has requested the information, identified its lawful authority and indicates that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law; or suspects that the information relates to national security or the conduct of international affairs; or is for the purpose of administering any federal or provincial law
- ?? To an investigative body named in the Regulations of the Act or government institution on the organization's initiative when the organization believes the information concerns a breach of an agreement, or a contravention of a federal, provincial or foreign law, or suspects the information relates to national security or the conduct of international affairs
- ?? If made by an investigative body for the purposes related to the investigation of a breach of an agreement or a contravention of a federal or provincial law
- ?? In an emergency threatening an individual's life, health, security (the organization must inform the individual of the disclosure)

⁶ Exceptions to Consent from the Guide For Business and Organizations, the Office of the Privacy Commissioner of Canada, p. 17 & 18

- ?? For statistical, scholarly study or research (the organization must notify the Privacy Commissioner before disclosing the information)
- ?? To an archival institution
- ?? 20 years after the individual's death or 100 years after the record was created
- ?? If it is publicly available as specified by the regulations
- ?? If required by law

TOOL: Refer to Section 3, Template 6.3b, for a Notice Form with a Consent Form. This can also be viewed as a ready-to-use WORD document at {[hyperlink](#)}.

c. Safeguards

Principle 7 requires that personal information be protected by security safeguards appropriate to the sensitivity of the information. It is the responsibility of the organization to protect personal information from loss or theft and to safeguard it from unauthorized access, disclosure, copying, use or modification. Personal information should be protected regardless of the format in which it is held.

Safeguard policies may include the following:

- ?? Physical measures (locked cabinets, restricting access to offices)
- ?? Safeguards for passwords
- ?? Reasonable Steps and Technology tools (firewalls, encryption, etc.)
- ?? Site Visits
- ?? Organizational Controls (limit access on a need-to-know basis)

TOOL: Refer to Section 3, Template 6.3 f, for Safeguard Policies. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

d. Need-to-Know

Individuals need to be assured that their information remains private and confidential and have a right to know who can access, view, use and disclose their personal information.

One of the challenges in the implementation of a privacy program is ensuring that only authorized staff has access to personal information and that this access is provided only on a need-to-know basis. If staff does not have a need-to-know, access to personal information should not be provided. Identifying and categorizing personal information in a manner that defines which staff can access which categories of personal information is difficult in long-term-care and community care where all providers have access to the complete file (all of the information all of the time). Security safeguards limit provider access to the record and may be difficult to put in place.

Limiting provider access to need-to-know personal information must be balanced with the evolving notion in the health care environment of the circle-of-care. The language “circle-of-care” suggests that the care giving is not an activity that involves isolated providers but rather an activity that involves a team of providers, as in long-term-care and community care, where all have the need to collect, use and disclose comprehensive personal information. Despite this, there must be assurances that personal information is being managed appropriately.

Carte blanche access to personal information introduces organizational risk.

In order to categorize personal information, questions must be asked of the personal information in the resident's/client's records. The following questions may assist in determining categories of information and which providers should access which categories.

- ?? Does the executive staff need access to all the personal information all the time?
- ?? Do physicians have a right to access all information, or only that of their own clients/residents?
- ?? Do nurses and case managers have a right to access all resident/client information in the organization or only that of their own residents/clients on any given day?
- ?? Are there specific categories of users who do not require access to clinical, social and financial information?
- ?? Are there specific categories of users who require read-only access to personal information?
- ?? Does the Ministry of Health and Long Term require any identifiable information on any resident or client?

If the organization has an information system with an electronic record, the system vendor should be approached to enable the authorized access policy, including the password protection for each of the categories of information so that users access only the category of information they are authorized for.

While this approach is desirable, it may not always be possible. In this case, the fall back position is the development of policy that providers and staff must follow regarding access to information on a need to know basis; meaning that staff should only access the information they require to do their job. Each staff member or provider should sign a confidentiality agreement, which should outline penalties if the staff person or provider disregards the access policy.

It should be noted that there may be times when it is essential for a staff person or provider to override the access policy. Such instances should be documented. An example would be when a professional assists in the treatment during a medical emergency, it may be necessary for the provider to access personal health information such as diagnosis, medications, lab work and other health information.

e. Employee Information

Employment records are not covered by PIPEDA unless the employer operates a federal work, undertaking or business (subject to Canada Labor Code).

Consent is not required to collect and use personal information for employment reasons. There is implied consent to collect and use information for employment reasons, including disclosing information to the benefits carrier. Employees should be informed of the employer's right to monitor email and internet use and the when video surveillance is used.

It is good practice to have employees sign confidentiality agreements. The signing of a Confidentiality Agreement is a process that reminds and binds staff to complying with privacy requirements. It is important that confidentiality agreements be signed by new staff as well as existing staff. Confidentiality agreements with existing staff should be updated annually as part of the employee review process.

TOOL: Refer to Section 3, Template 6.3 e, for a Template showing a Confidentiality Agreement. This can also be viewed as a ready-to-use WORD document at [{hyperlink}](#).

f. Staff Education

Staff Education is one of the most important components of the Privacy Program. All levels of staff, including the board, should receive education on the privacy principles and the organization's program as it is developed and implemented. Making Privacy a part of the orientation program and ongoing education will facilitate a privacy sensitive culture in the organization.

Staff education may include the following components:

- | | |
|------------------|---|
| Phase I | Privacy Principles and Legal Framework |
| Phase II | Posting the Privacy Review questionnaire for staff and inviting input
Review of the privacy review questionnaire at management meetings |
| Phase III | Review each aspect of the Privacy Plan as it is implemented: <ul style="list-style-type: none">/// Purpose of data collection/// Categories of personal information and access by role/// Obtaining informed consent as a process not just a form/// Limiting collection/// Guidelines for disclosure and retention of personal information/// Process for correcting and updating information/// Organization safeguards- use of ID, passwords, faxing other technical safeguards |

- ~~///~~ Process for individual access and requests for changes to personal information
- ~~///~~ Complaints process

Phase IV Post privacy checklist for employees
Privacy orientation for all new employees
Review privacy checklist results at staff meetings
Regular privacy education sessions throughout the year

TOOL: Refer to Section 3, 6.3 g, for a description of two PowerPoint presentations: Privacy and The 10 Principles, and Tips for Implementing a Privacy Program. These can be viewed as ready-to-use PPT presentations at {hyperlink} and {hyperlink}.

g. Third Party Contracts/Agreements

Organizations are responsible for privacy practices of third parties (such as physiotherapy, pharmacy, labs, agency) that directly or indirectly collect, use, store or disclose personal information. This also includes service companies that destroy or sanitize computer discs, hard drives, etc. Contracts must address the specific circumstances covered by each agreement. The organization's right to monitor/audit privacy practices of third parties needs to be incorporated into the contractual arrangements.

Long-term-care and community care will be responsible for the privacy practices of third parties that directly or indirectly collect, use, store or disclose personal information about the residents or clients. Contractual provisions must address the specific circumstances covered by each contract/agreement. Each contract/agreement where personal information is collected, used, disclosed or stored should require the third party e.g. service providers (labs, food services, physicians, pharmacies), etc. to comply with any privacy practices specified by the organization and PIPEDA. It is important that the organization monitor performance and enforce the agreement, including conducting periodic audits as provided in the contract.

If contracted third parties conduct activities and provide services that are commercial in nature, they are subject to PIPEDA. The third parties will be responsible for ensuring that they have privacy policies in place, that an individual has been designated responsible for privacy requirements, staff is educated on privacy, appropriate safeguards are in place.

Note that Third Party agreements must cover both compliance and confidentiality.

Long-term-care and community care organizations may request the third party to provide a letter outlining their compliance with privacy requirements. The receipt of such a letter from the third party may address the need of the long-term-care and community care organizations to develop contractual agreements with all of the third parties. The onus is on the third party to demonstrate its ability to comply with privacy requirements to the

satisfaction of the long-term-care or community care organization. It is recommended that legal counsel review these letters.

Provisions to be included in third party contracts/agreements are listed in the template in Section 3. Provisions in the template have been extracted from guidelines regarding third party contracts or data sharing agreements by:

- ?? The Office of the Information and Privacy Commissioner for Ontario, Model Data Sharing Agreement: Note that this site provides a template for data sharing agreements.
[http://www.ipc.on.ca/scripts/index .asp?action=31&P_ID=11281&N_ID=1&PT_ID=11271&U_ID=0](http://www.ipc.on.ca/scripts/index.asp?action=31&P_ID=11281&N_ID=1&PT_ID=11271&U_ID=0)
- ?? The Office of the Information and Privacy Commissioner for British Columbia, Guidelines are available for: http://www.oipc.bc.ca/public/guidelines_public.php
 - Information Access Research Agreements,
 - For Personal Information Exchange Agreements,
 - Data Services Contracts

TOOL: Refer to Section 3, 6.3 h, for text that is suitable for Third Party contracts. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

Where do third party contracts/ agreements apply?

- ?? Contracts with external providers such as laboratory services, pharmacy services, food services, dietitians, massage therapists, physiotherapists, etc. will require the inclusion of privacy protection language.
- ?? When individual personal health information is used for research purposes, an agreement for data sharing with the research body and or consultants should be acquired.

h. Confidentiality Provisions for Supplier Agreements

It is also recommended that suppliers sign a confidentiality agreement as part of the third party agreement process. Sample confidentiality provisions for agreements are shown in Section 3.

TOOL: Refer to Section 3, 6.3 i, for text that is suitable for Supplier Confidentiality Agreements as part of Third Party contracts. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

6.4 Phase IV – Sustaining the Gains

a. The Privacy Officer/Office Function

To sustain the gains of the privacy review, the privacy office should be in place and operational. The privacy office becomes responsible for the management and oversight of privacy practices throughout the organization. These responsibilities include:

- ?? addressing privacy questions, concerns and challenges to the organization and their third parties
- ?? ensuring the provision of ongoing privacy training for all staff
- ?? updating privacy policies
- ?? providing access by individuals to their personal information
- ?? managing disputes
- ?? performing audits (PIAs) on data repositories, systems and processes
- ?? managing events (e.g. breaches of privacy)
- ?? managing risk relating to privacy issues
- ?? ensuring third party contracts outline privacy requirements

b. Privacy Check-List

The privacy office may want to do an assessment of the status of privacy practices in the organization after implementation of the privacy plan. By completing a privacy check-list, organizations will be able to identify areas that require more work. The privacy check-list can be posted and used for regular educational purposes, discussions with staff and audits. Privacy is a journey and overtime, as staff becomes more sensitized to privacy issues, the organization will become more closely aligned with privacy requirements.

TOOL: Refer to Section 3, Template 6.4a, for a Privacy Check List. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

c. Communications Brochure

Principle 8 of the CSA Code states “an organization shall make readily available to individuals specific information about its policies and practices relating to the management of information”. Organizations that have implemented privacy programs should provide communication to stakeholders that describe the organization’s privacy practices. It is not advisable to publish privacy communications if the organization has not implemented a privacy program and is unable to respond to the expectations set in the brochure.

TOOL: Refer to Section 3, Template 6.4b, for a Communications Brochure. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

d. Handling Complaints

The CSA Code, in Principle 10, provides the ability for an individual to lodge a complaint. “An individual shall be able to address a challenge concerning compliance with the principles to the designated individual or individual for the organization’s compliance”. It is important for organization to have complaint procedures in place.

TOOL: Refer to Section 3, Template 6.4 c, for a procedure for Handling Complaints. This can also be viewed as a ready-to-use WORD document at {hyperlink}.

e. Privacy Policies

Privacy and policy go hand in hand. There will be an ongoing requirement by the privacy office to ensure the appropriate policies are in place. Policies for continuous review may include:

- ?? defining role-based access to the resident’s/client’s record by staff involved in care/service
- ?? allowing for sharing of client information between organizations for continuity of care/service
- ?? allowing for sharing identifiable information with contracted service organizations
- ?? defining a standard, logical and comprehensive format for the client’s record
- ?? accessing by a client to their own personal information
- ?? defining the process for refusal of access to a resident’s/client’s personal information
- ?? defining the process for the resident or client to make amendments to personal information. These should be signed and dated by the resident/client and added as an addendum. Where appropriate, third parties, such as insurance companies or legal counsel, should be advised of the noted disagreement
- ?? defining the process to investigate all complaints including who will conduct the investigation and how the investigation will be carried out, (e.g. who will be interviewed, who and how the findings will be documented)
- ?? defining the timelines for dealing with complaints (PIEPDA allows 30 days)
- ?? determining how complaints are referred to the Office of the Privacy Commissioner or other regulatory authority
- ?? outlining steps to be taken for implementing appropriate corrective action or measures, for example, amendment of policies and advising employees.
- ?? determining records retention periods and destruction methods

Section 3 – Implementation Tools

Phase I – Project Structure

6.1 a.	Template:	Job Description of a Privacy Officer	40
6.1 b.	Template:	Privacy Office Functions	41
6.1 c.	Spreadsheet:	Work Plan (Excel)	42
6.1 d.	Template:	Steering Committee Terms of Reference.....	43
6.1 e.	Template:	Sample Communications Bulletin	44

Phase II – Privacy Review

6.2 a.	Template:	Privacy Review Questionnaire.....	45
6.2 b.	Template	Gap Analysis	47
6.2 c.	Template:	Privacy Impact Assessment	48
6.2 d.	Template:	Risk and Mitigation Strategies	50
6.2 e.	Template:	Privacy Plan	52
6.2 f.	Template:	Organization-Wide Privacy Policies.....	53

Phase III – Implementation

6.3 a.	Template:	Notice	57
6.3 b.	Template:	Consent Form	62
6.3 c.	Template:	Letter for Fundraising Lists	64
6.3 d.	Template:	Confidentiality Policy and Agreement.....	65
6.3 e.	Template:	Safeguard Policies	67
6.3 f.	Presentation:	Staff Education (PowerPoint presentations)	69
6.3 g.	Template:	Third Party Contract	70
6.3 h.	Template:	Confidentiality Provisions for Supplier Agreements	72

Phase IV – Sustaining the Gains

6.4 a.	Template:	Privacy Check List	76
6.4 b.	Template:	Handling Complaints	79
6.4 c.	Brochure:	Sample Brochure.....	80

Phase I – The Project Structure

Template 6.1 a — (Refer to Section 2, Phase I)

For ready-to-use file go to {[hyperlink](#)}

Job Description for Privacy Officer

Overview

This individual shall be designated to lead the development of a privacy program for the organization, to oversee the ongoing development, implementation and maintenance of the organization's confidentiality, privacy and security related policies, procedures, guidelines and standards

This individual should oversee the identification, investigation and redress related to policy breaches.

The name and contact information of the privacy officer must be available upon request.

Proposed Qualifications:

- ?? Holds a senior leadership position in the organization, attends executive or senior management meetings and works full-time hours.
- ?? Has a good understanding of organization wide information practices; both internal and external flow of information, data collection tools and the information system
- ?? Have excellent communications and leadership skills.
- ?? Has experience in managing complex projects.
- ?? Does not have to be a full time position, can be responsibilities assigned to an existing role.
- ?? Needs the authority to implement the privacy program and respond to area where the standard is inadequate.
- ?? Needs access to resources.

Proposed Responsibilities:

- ?? Leads and manages the organization's privacy plan.
- ?? Chairs Privacy steering committee.
- ?? Leads the privacy office function for the organization, providing a centralized office or "resource center" for privacy expertise, consultation, and the resolution of privacy related issues.
- ?? Provides or coordinates support to each sub-office or facility as required throughout the initial project and on an ongoing basis.
- ?? Ensures adequate data protection practices are instituted for information that is managed internally and transmitted externally across the organization.
- ?? Establishes processes and standards for organization-wide privacy audits; including but not limited to the information system, business processes, and data collection tools, reviews results with the organizational governance team and front line staff as required.
- ?? Oversees the organization's privacy education program.

Privacy Office Functions

The privacy officer oversees the following privacy functions:

- ?? Coordinates regular review of privacy checklist
 - ?? Establishes regular audit process on information systems, business process and forms for authorized access and potential breaches of Privacy policy. (audit for consistency with the Privacy plan).
 - ?? Coordinates continuous Privacy education for staff and ongoing communications regarding the sustainability of a privacy culture.
 - ?? Coordinates the development, review and revision of privacy policy, providing input as required.
 - ?? Handles privacy complaints and the dispute mechanism for the organization – the organizational privacy officer may provide advice to the facility as required.
 - ?? Handles and tracks internal and external privacy queries

The Excel spreadsheet illustrated below is a template that can be adapted by organizations as they develop privacy work plans. Note: this illustration has been reduced to fit this space. It does not show all columns. Please refer to the original EXCEL file to view the full 11 month timeline.

**Draft High level work plan for Long Term Care and Community
ons in planning for each phase, timelines are only suggestions**

Task	Person Responsible	Time line (In weeks)						
		Month 1	Month 2	month 3	Month 4	month 5	Month 6	Month 7
Privacy Project								
Phase I Project Structure								
Appoint Privacy Officer	CEO/ED/							
Corporate Privacy Work Group TOR	Privacy Officer							
Revisions as needed to educational presentation	Privacy Officer							
Develop Work Plan for organization	Privacy Officer							
Education to corporate governance	Privacy Officer							
Meeting of Privacy Steering Committee (PSC)	Privacy Officer							
Revise Questionnaire for Privacy Review	PO and PSC							
Phase II Privacy Review and Develop the Plan								
Conduct a Privacy Review	Privacy Steering Cttee							
Review of data collection tools	Privacy Steering Cttee							
Document findings of Privacy	Privacy Steering Cttee							
Complete a Gap Analysis	Corporate Governance							
Conduct PIA as required								
Analysis of Privacy Review	Privacy Steering Cttee							
Develop the Privacy Plan								
Identify risks for gaps and risks	Privacy Steering Cttee							
Notice and Consent	Privacy Officer							
Third Party Contract	Privacy Officer							
Revision to P and P	Privacy Steering Cttee							
Development of new privacy practices/process	Privacy Steering Cttee							
Approvals	Corporate Governance							
Other								
Phase III Implementation								
Consent and Notice	Administrator/PO							
Policies	Administrator/PO							
Staff Education	Privacy Office							
Privacy Policy -	Administrator/PO							
Staff Agreements	Administrator/PO							
Third party contracts-lab pharmacy	Administrator/PO							
Audits	Administrator/PO							
Phase IV Sustaining the Gains								
Audits	Administrator/PO							
Ongoing Education	Administrator/PO							
Annual Review of Privacy Checklist	Administrator/PO							

Privacy Steering Committee Terms of Reference

Purpose:

To provide leadership to the organization in establishing a privacy program that is consistent with the Privacy standards and provides advice to the Privacy office on issues relating to Privacy program sustainability on an ongoing basis. May become part of an existing committee or the management team's terms or reference/responsibilities.

Responsibilities:

- ?? Review all available materials on Privacy
- ?? Receive education on Privacy requirements
- ?? Revise the Privacy Review questionnaire and oversee the administration of it.
- ?? Review of and inventory of all privacy related policies, data collection forms, information system
- ?? Analysis of results of the privacy review and gap analysis; identify risks and opportunities for improvement in relation to privacy as well as opportunities for streamlining and updating current practices and policies
- ?? Develop a Privacy plan for the organization
- ?? Develop education package specific to the needs of the organization (modify existing education templates)
- ?? Assist with education to all staff in the organization as required
- ?? Provide input into customizing the Organizational Privacy Policies, third party contract, notice and consent and communications templates.
- ?? Facilitate execution of the communications plan
- ?? Develop a complaints resolution process for the facility and ensure review with residents and or family council
- ?? Support the implementation of the privacy compliance plan

Meetings: Initially every 2-3 weeks for 4- 6 months then monthly.

Accountability: to the individual assigned lead responsibility for Privacy

Potential Membership:

Administrator/ Executive Director
 Privacy Officer (if different than the administrator)
 Director of Care/Client Service Manager/Clinical Leader/Designate
 Program Manager
 Educator
 Office Manager/ Bookkeeper
 Clinical staff

Minutes: Action items and decisions to be recorded.

*The steering committee may create working groups to address key components of a privacy program such as education and communications.

Initial Communications

Template 6.1 e — (Refer to Section 2, Phase I)

For ready-to-use file go to {hyperlink}

Sample communications bulletin

The _____(organization name) has always been committed to keeping client/resident personal information accurate, confidential, secure and private. In an era where technology enables unlimited access to personal information within and across organizations, it is essential to revisit existing practices and procedures and update them as needed. To this end, we are in the process of enhancing our information management practices. Our process of enhancement has been enabled by privacy requirements that are based on 10 privacy principles which are internationally accepted.

We are pleased to inform you that we are revitalizing our privacy practices and developing a plan, consistent with the privacy principles. These principles provide a privacy framework for the management of personal information. By implementing this privacy framework, our organization will be better positioned to provide greater privacy protection of personal information.

We are pleased to announce that the Privacy Implementation Project will be led by: _____ (the project lead's name and title).

We have appointed a privacy steering committee to coordinate the Privacy activities. Members of the steering committee include:

Watch for regular updates on the Privacy Project. We will keep you informed of our progress and look forward to your contributions to this important project.

Phase II – Privacy Review

Privacy Review Questionnaire

The privacy review is the most important component of the privacy project and one of the main activities to be undertaken by the privacy steering committee.

There are a variety of tools that may be used to facilitate the privacy review. A simplified version of a privacy questionnaire can be completed on line at:
www.priva-c.com/privacysource/tools.asp

The Office of the Information Privacy Commissioner for Ontario also provides an initial privacy review tool at www.ipc.on.ca. Go to search and enter Privacy Diagnostic Tool.

A Privacy Questionnaire template is provided to serve as a guideline for organizations to follow. The template facilitates a review of information management practices pertinent to the 10 privacy principles. To conduct a privacy review the steering committee should:

1. Customize the questionnaire (template).
2. Answer the questionnaire for the organization or by department
3. Document the results
4. Complete a Gap Analysis or Privacy Impact Assessment on the findings

Template 6.2 a — (Refer to Section 2, Phase II)

For ready-to-use file go to {hyperlink}

Privacy Review Questionnaire

Information Collection

- ?? What kind of personal information is collected by your department/organization?
- ?? Identify all collection forms including electronic forms if applicable
- ?? Categorize the information into main categories such as:
 - ?? Financial, Clinical, Social, Demographic
- ?? For each collection form, how is the personal information managed once it is collected?
- ?? How and where is personal information that is collected on residents kept on a day- to- day basis?
- ?? Who is responsible for deciding what information is collected and how it is collected?
- ?? For each collection form identify if the collection is: from the client/resident from other organizations

Purpose

- ?? Have you identified the purposes for each category of personal information?
- ?? Who uses it and for what purpose?
- ?? Are these purposes identified at or before the time of the information is collected?

- ?? Do you collect only the personal information needed for the identified purposes?
- ?? Do you document the purposes for which personal information is collected?
- ?? If you gather and combine personal information from more than one source, do you ensure that the original purposes have not changed
- ?? Are residents/clients (SDMs) aware of the purposes for collection?
- ?? Is all of the information collected required?

Use

- ?? How is personal information that is collected by each of the collection forms used?
- ?? Identify all uses for the collection of personal information for each collection form.
- ?? Identify each user of the personal information collected for each collection form.

Disclosure

- ?? To whom (individuals/organizations) is the personal information disclosed (inside and outside the organization)?
- ?? Identify the purposes for disclosure of personal information outside the organization.
- ?? Are residents (SDMs) aware of the purposes for disclosure of the information collected on the form outside the organization?
- ?? Identify how personal information that is collected on the collection form is disclosed outside the organization?
- ?? List the policies that define disclosure of information that is collected on the collection form outside the organization.

Retention

- ?? Have you developed a timetable for retaining and disposing of personal information?
- ?? When you no longer require personal information for the identified purposes or it is no longer required by law, do you destroy, erase or make it anonymous?
- ?? How and where is personal information stored that is no longer actively in use?
- ?? How is personal information destroyed?

Policies

- ?? Do you have policies and procedures in place that apply to your collection of personal information practices?
- ?? Identify all policies that define personal information collection practices by collection form if they are available.
- ?? Identify Consent policies.

Safeguards

- ?? Review physical, technological and organizational security measures
- ?? Do these measures adequately prevent improper access, modification, use, disclosure and or disposal of personal information?
- ?? Is your personal information protected by security safeguards that are appropriate to the: sensitivity of the information, method of storage?
- ?? Review of the "need-to-know" by staff role for each category of information
- ?? Has your staff been trained about security practices to protect personal information?
- ?? Is your staff aware that they should properly identify individuals and establish their right to access the personal information before disclosing it?
- ?? Do you have rules about who is permitted to add, change, or delete personal information?

- ?? Is there a process and accountability in the organization that assigns user accounts, access rights and security authorizations?
- ?? Do you ensure that no unauthorized parties may dispose of, obtain access to or modify or destroy personal information?
- ?? What is the process for removing users when they leave the organization or go on leave?

Gap Analysis

Once the Privacy questionnaire is answered, gaps in privacy practices need to be identified. Based on the steering committee's knowledge of the CSA Code, most gaps in privacy practices will be obvious. A plan should be developed to close these gaps, e.g. provide education, develop policy, etc. In most cases, the gap analysis can likely be completed after the privacy questionnaire is completed.

The following web site may be of assistance in conducting the Gap Analysis.

Priva-C: www.priva-c.com/privacysource/tools.asp

TOOL: Template 6.2 d, Risk and Mitigation Strategies (Gap Analysis Template), can be used to facilitate the gap analysis (but steps 1- 3 may not be necessary).

Some gaps may be more difficult to identify, such as those associated with information systems and data repositories. When it is difficult to clearly identify the gaps, the committee may consider conducting a Privacy Impact Assessment on these components of their information management practices. When a PIA is conducted, a comprehensive gap analysis is also completed. Where a PIA is required the 5 steps should be followed:

1. Inventory of personal information practices
2. Flow chart of key processes
3. Apply the Privacy Principles
4. Privacy Analysis
5. Risks and Mitigation Strategies

Privacy Impact Assessment

The privacy review questionnaire and gap analysis will assist in determining if a Privacy Impact Assessment (PIA) is required. The initial steps of the PIA have already been completed through the privacy questionnaire.

Step 1: Inventory

The business processes that involve the handling of personal information and activities within the process are documented.

Business Process	Activity within Process	Personal Information that is or may be Collected
Admission	Signing admission agreement	
	Review admission package	
	Collection of personal health information	Physical Social Financial Spiritual
	Enter client information into computer system	
	Etc.	

Step 2: Create a Diagram

A diagram that shows the flow of information associated with each business process is helpful to complete a thorough privacy analysis.

A diagram depicts how personal information can make its way through a system and depicts some subsequent business processes in a way that can be tracked and analyzed with respect to how information is used, to whom is it disclosed and who has access to it, etc.

The diagram facilitates the identification of the need for security safeguards. Questions to ask of an information system may include:

- ?? Are safeguards in place for the repository?
- ?? Can only authorized providers “that need-to-know” access the system?
- ?? Is there a means of logging who has accessed the data repository and when access occurred?
- ?? Is the log of accesses monitored?
- ?? Is the data repository encrypted or should it be.
- ?? Are appropriate firewalls in place?

Step 3: Do Privacy Principles Apply?

Based on the inventory of business processes and activities provided in step 1 and the business process mapped in step 2 an analysis is required to identify if information being collected, used or disclosed is personal in nature. If the information is personal, privacy principles will apply.

Business Process	Activity within process	Personal Information that is or may be Collected	Do Privacy Principles Apply?
Assessment	Data collection Incoming Information, (e.g. inquiries from the individual or SDM)	Medical History Life History Religion Family Contact information Previous treatment Diagnoses Medications taken	Yes

Step 4: The Privacy Analysis/Asking Privacy Questions

The privacy analysis involves questioning each business process and activity against the privacy principles. If there is a “no” to a privacy principle question there is a gap in meeting privacy standards.

Business Process	Activity within process	Personal Information that is or may be Collected	Privacy Principle Questions	Gap in Privacy Yes or No
Assessment	Data collection	Religion	Identifying purpose	Y
Etc.				

Step 5:
Identify Privacy Risks, Assess the Risks and Define Mitigation Strategies

Next, a risk assessment is undertaken based on the conclusions and privacy gaps identified during Step 4. The gaps are assigned a risk of high, medium or low. A risk is high when privacy standards are not met and a breach, complaint or challenge is possible. The risk is low when the privacy principle is adequately addressed and it is unlikely that there will be a complaint or a challenge. Along with the risk assessment, an action (mitigation strategy) should be identified that would eliminate the risk.

Risks and Mitigation Strategies (GAP Analysis Template)

Gap in CSA Principle	Risk	Risk Level	Mitigation Strategy
Accountability	Absence of privacy policies could lead to mismanagement of client information and result in complaints or challenges	High	Privacy policies must be developed
Identifying Purpose	Failure to identify the purposes for collecting personal information may lead to complaints and challenges	High	Purposes for the collection of information will be documented in the notice and in policy and communicated by staff
Consent	Express consent is not obtained for the collection and disclosure of personal information	Medium	Institute the notice and informed consent
Limiting Collection	Forms are duplicated; several disciplines collect the same information. Information received from CCAC is recollected	Medium	Review of forms and information collected on each
Limiting Use, Disclosure, Retention	Personal information is generally used, disclosed and retained for the delivery of care and services	Low	Staff education on the principles will serve as a reminder.
Accuracy	Processes are in place to update personal information and to identify and make corrections in the event of error	Low	Continue current practices
Safeguards	Some users have remote access to information system Passwords are not regularly renewed	High	Security for remote access to be reviewed with vendor.
Openness	Information is not readily available on policies related to personal information	Medium	Organizational Privacy Policy will be developed and posted
Individual Access	There is no process in place to inform individuals of the existence, use and disclosure of personal information and for individuals to request access to this information	Medium	Information to be included in the admission process. Staff education
Challenging Compliance	Complaints procedures do not exist	Medium	Complaints process to be developed and posted.

PIA Methodologies

Other methodologies available for conducting PIAs are available from the following web sites:

- ?? The Alberta Medical Association provides Guidelines to conduct a PIA in a physicians office:
http://www.albertadoctors.org/advocacy/healthinfo/privacy_impact_statements.htm
- ?? The British Columbia Office of the Information and Privacy Commissioner has a PIA methodology: <http://www.oipc.bc.ca/public/pia/>
- ?? Management Board Secretariat of Ontario has a PIA Methodology/Guidelines:
<http://www.gov.on.ca/MBS/english/fp/pia/index.html>
- ?? The Ontario Office of the Information and Privacy Commissioner has a Privacy Diagnostic Tool which provides guidelines for a preliminary PIA: www.ipc.on.ca search on Privacy Diagnostic Tool
- ?? Treasury Board of Canada Secretariat has introduced a PIA eLearning tool:
http://www.cio-dpi.gc.ca/pgol-pged/index_e.asp

Privacy Plan

Once the Privacy Questionnaire is completed and results analyzed, using the PIA methodology or Gap Analysis, a plan can be developed which will include identifying all of the risk mitigation strategies and actions, sub-activities, timelines and responsibilities for completion. MS Project, Excel or Word can be used to develop and track project plans. A simple template may be all that is required building on the gap analysis. Once the plan is developed and approved, it may be necessary to assign resources and implementation can begin.

Template 6.2 e — (Refer to Section 2, Phase II)

For ready-to-use file go to {hyperlink}

Draft Privacy Plan

Gap in CSA Principle	Action	Time	Lead
Accountability	Approval of organization-wide privacy policy		
Identifying Purpose	Identify purpose in brochure, notice and consent		
Consent	Institute Express consent at the time of admission. Get consent for existing clients/residents		
Limiting Collection	Revision to x forms and develops policy for the revision and development of new forms.		
Safeguards	Implement practice of a 90 day password change Education and policy for removing users from system access. Restrict access to some categories of information by staff role (need to know)		
	Etc.		

Organization-Wide Privacy Policies

Policy is an area of organizational vulnerability, and organizations are therefore advised to obtain legal advice. Once policy is posted the organization becomes legally liable if it fails to abide by the privacy policy statements. Publish privacy policy only when you can confirm that your organization is adhering to the privacy principles declared.

Organization-Wide Privacy Policies

Principle 1 - Accountability

The _____ 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.

- 1.1 The owner/or chief executive officer of the _____ has ultimate accountability for protecting the personal information of clients and residents. The owner/chief executive officer may be supported in this activity by delegating the day-to-day operational privacy responsibilities to another individual(s). All staff share responsibility for adhering to the _____ organization's privacy policies and procedures.
- 1.2 The name and contact information the individual(s) designated by the _____ to oversee the _____ compliance with the principles is available upon request.
- 1.3 The _____ is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The _____ will use contractual or other means to provide a comparable level of protection while the information is being processed by the third party.
- 1.4 The _____ shall implement policies and practices to give effect to this policy, including
 - (a) implementing procedures to protect personal information;
 - (b) establishing procedures to receive and respond to complaints and inquiries;
 - (c) training staff and communicating to staff information about the _____

Principle 2 - Identifying Purposes

The purposes for which personal information is collected shall be identified by the _____ at or before the time the information is collected. The primary purposes are the delivery of care and services, quality management, research, billing, and meeting legal and regulatory requirements.

2.1 Identifying the purposes for which personal information is collected at or before the time of collection allows the _____ to determine the information they need to collect to fulfill these purposes.

2.2 The identified purposes are specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An admissions or application for services form, for example, may give notice of the purposes.

2.3 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.

2.4 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

Principle 3 – Consent

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

Note: *In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Acquiring consent may be impossible or inappropriate when the individual is cognitively impaired, seriously ill or psychotic and the substitute decision maker is not available. Organizations are advised to follow the rules provided in the Health Care Consent Act and Substitute Decisions Act.*

3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, the _____ will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when the _____ wants to use information for a purpose not previously identified).

3.2 The principle requires “knowledge and consent”. The _____ shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such

a manner that the individual can reasonably understand how the information will be used or disclosed.

3.3 The _____ as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

3.4 The form of the consent sought by the _____ may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, the _____ shall take into account the sensitivity of the information.

3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual seeking service/admission should reasonably expect that the _____, in addition to using the individual's name and address for administration purposes, would also contact the individual to advise on the availability of the room in the facility. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

3.6 The way in which the _____ seeks consent may vary, depending on the circumstances and the type of information collected. The _____ will generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative. Organizations are advised to follow the rules for an authorized representative provided in the Substitute Decisions Act.

3.7 Individuals can give consent in many ways. For example:

- (a) an admission form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
- (b) a check-off box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
- (c) consent may be given orally when information is collected over the telephone; or (d) consent may be given at the time that individuals use an organization's product or service.

3.8 An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The _____ will inform the individual of the implications of such withdrawal.

Principle 4 - 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.

4.1 The _____ shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to

fulfil the purposes identified.

4.2 The requirement that personal information be collected by fair and lawful means is intended to prevent the _____ from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

Principle 5 - 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.

5.1 If the _____ uses personal information for a new purpose, it will document this purpose.

5.2 The _____ will should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines will include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. Organizations and long-term-care facilities are subject to legislative requirements with respect to retention periods. In Ontario, retention periods are not defined for long-term-care facilities and community care organizations.

5.3 Personal information that is no longer required to fulfil the identified purposes will be destroyed, erased, or made anonymous. The _____ will develop guidelines and implement procedures to govern the destruction of personal information.

Principle 6 – 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.

6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

6.2 The _____ facility will not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, will generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

Principle 7 - Safeguards

Security safeguards appropriate to the sensitivity of the information will protect personal information.

7.1 The security safeguards will protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The _____ will protect personal information regardless of the format in which it is held.

7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.

7.3 The methods of protection should include:

- ?? physical measures, for example, locked filing cabinets and restricted access to offices;
- ?? organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
- ?? technological measures, for example, the use of passwords and encryption.

7.4 The _____ will make their employees aware of the importance of maintaining the confidentiality of personal information.

7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information

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.

Principle 8 – Openness

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

8.1 The _____ will be open about their policies and practices with respect to the management of personal information. Individuals should be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

8.2 The information made available shall include:

- ~~the~~ the name/title and address of the person (privacy officer) who is accountable for the _____ policies and practices and to whom complaints or inquiries can be forwarded;
- ~~the~~ the means of gaining access to personal information held by the _____
- ~~a~~ a description of the type of personal information held by the _____

- _____ , including a general account of its use;
- ~~///~~ a copy of any brochures or other information that explain the _____ policies, standards, or codes; and
- ~~///~~ what personal information is made available to related organizations (eg, other healthcare providers).

8.3 The _____ may make information on its policies and practices available in a variety of ways. For example, The _____ may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

Principle 9 - 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.

Note: *In certain situations, the _____ may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.*

9.1 Upon request, the _____ will inform an individual whether or not the organization holds personal information about the individual. The _____ will indicate the source of this information. The _____ will allow the individual access to this information. However, the _____ may choose to make sensitive medical information available through a medical practitioner. In addition, The _____ will provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

9.2 An individual may be required to provide sufficient information to permit the _____ to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

9.3 In providing an account of third parties to which it has disclosed personal information about an individual, the _____ will attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the _____ will provide a list of organizations to which it may have disclosed information about the individual.

9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, The _____ will amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge should be recorded by the _____. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

Principle 10 - Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Note: The individual will be able to address a challenge concerning compliance with the above principles to the owner or chief executive officer.

10.1 The _____ will put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint process should be easily accessible and simple to use.

10.2 The _____ will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint mechanisms. A range of these mechanisms may exist.

10.3 The _____ will investigate all complaints. If a complaint is found to be justified through the internal or external complaint review process, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

Phase III – Implementation

Notice

This proposed notice offers an example for organizations to follow. It is assumed that legal counsel will review the contents of the notice and may make changes to it prior to its use.

Template 6.3 a — (Refer to Section 2, Phase III)

For ready-to-use file go to {hyperlink}

Notice

Keeping Your Personal Information Private is Important to Us

The _____ (name of organization) provides you with a broad variety of care services. To meet your needs and serve you well, the _____ (name of organization) needs to know personal information about you.

You, as an individual, have a right to know how we collect, use and disclose personal information. You have a right to expect that, to the best of our ability, your personal information held by us remains accurate, confidential and secure.

The _____ (name of organization) is proud of its long standing commitment to maintaining the confidentiality and security of personal information and has implemented practices to better protect the privacy of your personal information

The _____ (name of organization) collects, uses, discloses and stores facts about you and your health.

These facts are collected to help provide health care or payments for health care. They include:

- ?? Your name, address, and your Ontario Health Care number.
- ?? Facts about your health, health care history and the health care that you have been given.
- ?? Facts about payment for your health care.

We use this information and share it only with those who need to know that information. For instance, we might use it to:

- ?? To make decisions about the types of services you need
- ?? To serve as a means to communicate with other service providers
- ?? To monitor the provision of services and evaluate your response to services provided
- ?? For administration, management, strategic planning, decision-making, research, allocating of resources within the organization.
- ?? To meet legal and regulatory requirements

Note: We may also use your name and address as part of the organization's fund raising activities

These are your rights:

- ?? You may see or have access to your personal health information.
- ?? You may ask for and receive any copy of your health record.
- ?? You may ask us to correct your records.
- ?? Your personal information is private. Unless sharing it with others is authorized by law, we cannot and will not give out any of your personal information without your consent.
- ?? You may make a complaint to our Privacy Officer about access to your personal information, or about how it is collected, stored, used or disclosed to others.

If you would like to know more about how your personal information is collected, used, stored, and disclosed, ask the staff that are caring for you, or contact the _____organization's Privacy Officer at _____ tel. number.

Consent Form

Note: This proposed Consent form, appended to the notice, offers an example for organizations to follow. It is assumed that legal counsel will review the contents of the Consent form and may make changes prior to its use.

Template 6.3 b — (Refer to Section 2, Phase III)

For ready-to-use file go to {hyperlink}

Notice and Consent

Keeping Your Personal Information Private is Important to Us

The _____ (name of organization) provides you with a broad variety of care services. To meet your needs and serve you well, the _____ (name of organization) needs to know personal information about you.

You, as an individual, have a right to know how we collect, use and disclose personal information. You have a right to expect that, to the best of our ability, your personal information held by us remains accurate, confidential and secure.

The _____ (name of organization) is proud of its long standing commitment to maintaining the confidentiality and security of personal information and has implemented practices to better protect the privacy of your personal information.

The _____ (name of organization) collects, uses, discloses and stores facts about you and your health.

These facts are collected to help provide health care or payments for health care. They include:

- ?? Your name, address, and your Ontario Health Care number.
- ?? Facts about your health, health care history and the health care that you have been given.
- ?? Facts about payment for your health care.

We use this information and share it only with those who need to know that information. For instance, we might use it to:

- ?? To make decisions about the types of services you need
- ?? To serve as a means to communicate with other service providers
- ?? To monitor the provision of services and evaluate your response to services provided
- ?? For administration, management, strategic planning, decision-making, research, allocating of resources within the organization.
- ?? To meet legal and regulatory requirements

Note: We may also use your name and address as part of the organization's fund raising activities

If you do not wish to have your information used for fundraising purposes, initial here: _____

These are your rights:

- ?? You may see or have access to your personal health information.
- ?? You may ask for and receive any copy of your health record.
- ?? You may ask us to correct your records.
- ?? Your personal information is private. Unless sharing it with others is authorized by law, we cannot and will not give out any of your personal information without your consent.
- ?? You may make a complaint to our Privacy Officer about access to your personal information, or about how it is collected, stored, used or disclosed to others.

If you would like to know more about how your personal information is collected, used, stored, and disclosed, ask the staff that are caring for you, or contact the _____organization's Privacy Officer at _____ tel. number.

CONSENT

I, _____, have reviewed the above summary of information relating to the Organization's Privacy Policy. I have had an opportunity to have questions answered regarding this Notice and feel that I have a reasonable understanding of the Notice. I hereby authorize the collection, use and disclosure of my personal information by the organization in order to facilitate the provision of care and service to myself and for specific, related purposes as detailed within that Notice.

Resident/Client Name (Print):

OHIP:

OR

DOB (mm/dd/yy):

/

/

Resident/Client Signature:

Date Signed (mm/dd/yy)

/

/

* If Resident/Client is unable to sign:

Name of Substitute

Decision Maker, SDM (Print)

Relationship:

Signature of SDM::

Date Signed (mm/dd/yy)

Name of Witness to Signature of SDM (Print:):

Signature of Witness to Signature of SDM:

Template Letter for Fundraising Lists

[Click **here** and type Organization Name]

I am writing to advise you that your name and contact information is currently on our foundation list for the purpose of fundraising. Fundraising is an important component of our activities. It enables us to enhance services provided to our residents and clients. We do regular fundraising for the purpose of XXX and often send letters to potential donors, such as you, requesting their support. We value your support and hope that you may want to continue to enable our fundraising endeavors.

If you would like us to remove your name from our fundraising lists, kindly check the box below and return this letter to us in the envelope attached. If you prefer, you can contact _____ (contact person's name) at _____ (contact person's phone number) at any time and ask that your name be removed from our fundraising lists.

We thank you for any support you have provided in the past.

Confidentiality Policy and Agreement

Confidentiality Policy

Clients/residents have the right to protection of all their personal information. Each organization must support the client's/resident's right to privacy. Staff in the organization must be committed to maintaining the privacy and confidentiality of clients and residents and their associated personal and personal health information. Breaches of privacy place the organization at risk.

A condition of employment in the organization is that all employees sign a confidentiality agreement. This agreement will be placed in the employee's file. This agreement will be renewed at regular intervals, (with the annual performance review). Failure to hold the personal information of clients and residents confidential and private may lead to disciplinary action which may include termination of employment.

Breaches of confidentiality include accessing personal information without authorization to do so and without a need-to-know.

Sample Employee Confidentiality Agreement

Name of organization _____

Name of employee _____

I acknowledge that during my employment with the _____ organization that I will have access to personal information about clients and residents, their families, and other employees which is of a private and confidential nature.

At all times I will respect the privacy of clients and residents, their families, and other employees.

I will treat all _____ organization's clinical, administrative and financial information about clients and residents, their families, and other employees as confidential information.

I will ensure that private and confidential information is not inappropriately accessed, used or disclosed either directly by me or by virtue of my password to systems.

I understand that violations to privacy and confidentiality may include but are not limited to:

- ?? Accessing personal information that I do not require for work purposes.
- ?? Misusing or disclosing personal information without proper authorization.
- ?? Altering personal information of residents and clients or other employees.
- ?? Disclosing to another person my user name and password to enable unauthorized access to personal information

I will only access, use and transmit private and confidential information using organization authorized hardware, software or other equipment, as required by the duties of my position

I understand and agree to abide by the conditions outlined in this agreement which will remain in force even if I cease to have an association with the _____ organization.

I understand that if any of these conditions are breached, I may be subject to disciplinary action that may include termination of employment.

Name (please print) _____, Signature _____, Date _____

Name of Witness (please print) _____, Signature _____

Draft Policies – Safeguards

Policy: It is the policy of x to implement and maintain physical measures and safeguards for passwords to prevent unauthorized access to personal information.

Physical Measures

- ?? Identification badges are worn by all staff, volunteers and providers at all times.
- ?? Old records and thinned charts will be locked in the designated location at all times.
- ?? Filing cabinets that contain personal information will be locked when not in use.
- ?? Active records are closed and placed on the chart rack when not in use.
- ?? Doors that provide entry to areas where there is sensitive information (health records) will be locked when there is no provider in the area.

Passwords

- ?? All systems users are responsible for their confidential password.
- ?? The information system stores passwords in a file that is encrypted, that can not be read.
- ?? Password characters are never displayed on monitors, or available to anyone (post-it notes, etc).
- ?? Passwords are keyed in by the user each time the user signs on.
- ?? Passwords should be a minimum of 6 characters long and include a combination of alpha and numeric characters.
- ?? Passwords are changed by users every 90 days and recently used passwords cannot be re-used.

Technological

- ?? All print outs of resident or client information are disposed of securely when no longer required.
- ?? Users log off the system when a session is finished.
- ?? The information system automatically ends a session after x minutes of inactivity.
- ?? Virus software is updated routinely.
- ?? Operating systems are updated with patches as they become available from the vendor.
- ?? Sensitive and confidential files are encrypted for transmission purposes
- ?? Firewalls are in place.
- ?? A disaster plan is in place and data recovery is possible at all times.
- ?? Measures are taken to prevent visitor viewing of computer screens.

Faxing

- ?? It is the policy of _____ (name of organization) to ensure that faxing of personal information is done only when it is required urgently. Personal information, that is not urgently required, should be sent by regular mail and marked as confidential.

- ?? Personal information that is faxed to third parties is faxed in a secure manner, e.g. the person on the receiving end is notified prior to sending the confidential fax
- ?? Fax machines should be located in non-public areas
- ?? A confidential cover sheet should be attached to all faxes

Draft wording for fax cover sheets:

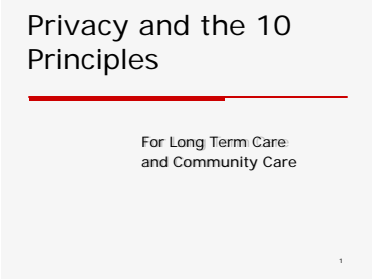
The attached fax contains confidential information that must not be disclosed to anyone other than the intended recipient. If you receive this fax in error, please notify _____ (number of sending organization) immediately.

Staff Education

The title slides for two PowerPoint presentations. Each contains 27 slides are shown below.

6.3 e (i)

The first, *Privacy and the 10 Principles*, is an overview of the privacy principles and requirements, ideally suited for audiences who are being introduced to privacy concepts for the first time. It provides information on the underlying privacy principles (the CSA Code) and applicable legislation.




Privacy and the 10 Principles

For Long Term Care
and Community Care

6.3 e (ii)

The second, *Tips For Implementing A Privacy Program*, is a summary of the implementation phases in section 2 of the tool kit. Target audiences might include organization governance, the privacy steering committee and components may be useful for staff. It covers all phases of implementation and introduces the audience to all key topics listed in the Table of Contents.



Tips to Implementing a
Privacy Program

For Long Term Care and
Community Care

Third Party Contracts- Potential Provisions

The following information should be included in third party contracts.

The Organization's Privacy Policy and Procedures

Identify the requirement that all personal information provided by the disclosing party to the collecting party shall continue to meet or exceed the level of data protection of the disclosing party. Ensure that the collecting party shall adhere to the disclosing party's privacy policy, e.g. appoint a knowledgeable senior person to be responsible for privacy compliance, train staff on privacy requirements, etc.

Definitions

Provide definitions of any terms which may be unique to the subject matter, or which may not be common knowledge e.g. program terms, acronyms, etc.

The purposes Personal Information to be Shared

List all elements of personal information that will be disclosed and the purpose for the disclosure of each element. Also identify the frequency of the disclosure along with the medium for the disclosure, e.g. encrypted mail, disk, secured fax, etc.

Uses of the Shared Information

List the specific use(s) of the personal information. Identify that the collecting party shall not use the personal information provided for any other purposes.

Accuracy and Completeness of the Shared Information

Identify the steps and measures to be taken to ensure that the information disclosed is accurate and complete.

Disclosure Practices for the Shared Information

Identify that all information shared shall not be further disclosed by the collecting party without explicit written authorization of the disclosing party.

Data Retention and Destruction for the Shared Information

Identify the start and termination dates for the agreement/contract.
Identify the length of time the personal information will be retained by the collecting party.
Identify archival and destruction requirements.
State whether the disclosure/collection will be a one-time occurrence, time limited or ongoing.

Security of the Shared Data

List the security controls that must be in place prior to the commencement of the disclosure. Security controls include:

- ?? Ensuring the security and completeness of transmission.
- ?? Ensuring that only the required personal information will be transferred.
- ?? Ensuring that personal information will be processed in a complete and accurate manner (audit trails and/or management reports produced).

Individual Access to information

Identify the process by which individuals can access their own personal information in the possession of the collecting party.

Investigations of a Complaint

Identify the process that requires the collecting party to co-operate with and assist in any investigation of a complaint that personal information has been used or disclosed contrary to privacy policies.

Access to the collector's premises

Identify the right of access of the disclosing party to the collector's premises:

- ?? to recover any and all of its records and
- ?? for auditing purposes to ensure compliance

Monitoring and Enforcing Compliance

Identify remedies for violation such as:

- ?? dispute resolution
- ?? determining appropriate remedies if the collector is in breach

Audits

Identify the right of the disclosing party to audit, or have a third party audit, the privacy policies and practices of the collecting party.

Sample Confidentiality Provisions for Supplier Agreements

ARTICLE 1. CONFIDENTIAL INFORMATION

1.01 Any information, including but without limiting the foregoing, any and all information relating to the _____ (organization name) including Personal Health Information of its clients/residents, or otherwise proprietary to _____ (organization name) issued to, used by or disclosed to or developed by _____ (name of supplier company) in connection with the performance of the Agreement are confidential (“Confidential Information”).

1.02 _____ (name of supplier company) shall not, without the prior written consent of the _____ (organization name), disclose the _____ (organization’s name) Confidential Information to any person or entity except to its employees who require same in connection with performing _____ (name of supplier company) obligations under this Agreement, and who agree to act in compliance with the confidentiality obligations set out in this Agreement and _____ (name of supplier company) Privacy Code.

1.03 On completion or termination of this Agreement for any reason, _____ (name of Supplier Company) shall forthwith return to the _____ (organization name) all the Confidential Information either obtained or developed in the course of this Agreement. _____ (name of Supplier Company) obligations with respect to Confidential Information shall survive the expiration or other termination of this Agreement for any reason.

ARTICLE 2. PROTECTION OF PERSONAL HEALTH INFORMATION

General

2.01 In addition to Article 1 above, which applies to Confidential Information generally, there are additional obligations required with respect to Personal Health Information as set out below which the Parties shall comply with.

2.02 The parties acknowledge that this Agreement is intended in good faith to meet the requirements set out in all applicable legislation and regulations dealing with the protection of Personal Health Information and acknowledge that they shall work together to ensure that any new privacy legislation introduced by Ontario, shall be complied with.

2.03 The _____ (name of Supplier Company) and the _____ (name of organization) shall be responsible for ensuring compliance with the provisions of this Agreement for the protection of Personal Health Information.

The _____ (name of Organization)

2.04 The _____ (organization name) acknowledges that it is aware of the current rules governing the confidentiality of personal health information pursuant to applicable legislation and regulations there under. The _____ name of organization) further acknowledges that its obligations under such legislation and regulations are not obviated by entering into this Agreement and engaging the services of (name of Supplier Company).

The _____ (name of supplier company)

2.05 _____ (name of supplier company) shall fulfil the same confidentiality obligations that apply to the _____ (name of organization) in respect of _____ (name of supplier company)'s provision of Services under the Agreement.

2.06 _____ (name of Supplier Company) shall be entitled to use the Personal Health Information provided by the _____ (name of organization) solely for purposes of providing the Services and for no other purpose whatsoever.

2.07 _____ (name of Supplier Company) shall ensure that its employees are aware of and agree in writing to be bound by the confidentiality provisions that are set out in this Agreement.

2.08 A breach of the confidentiality provisions by any of employees of _____ name of Supplier Company) shall be grounds for immediate dismissal. Neither _____ (name of Supplier Company) nor its employees shall provide access to or use, disclose or dispose of any Personal Health Information except in accordance with the provisions of this Agreement.

Confidentiality Safeguards

2.09 In order to safeguard the confidentiality of the Personal Health Information that are transferred by the _____ (name of organization) to _____ (name of supplier company), the following procedures shall be followed:

(a) Transfer of Data:

(i) All original personal health information shall remain at the _____ (name of organization).

2.10 The _____ (name of organization) shall ensure that it limits its transfer of Personal Health Information to _____ (name of Supplier Company) to that which is necessary for the provision of Services under this Agreement.

(i) The parties commit to safeguarding the confidentiality of the Personal Health Information through jointly approving the processes to be used to transfer _____ (name of organization) data to _____ (name of Supplier Company) and back to _____ (name of organization).

(ii) _____ (name of Supplier Company) shall destroy the Personal Health Information confidentially in a manner agreed to by the parties or return it to the _____ (name of organization) within ___ days of the completion of the Services on the information. No Personal Health Information shall be retained by _____ (name of Supplier Company).

(b) Access to Data

(i) _____ (name of supplier company) shall institute confidentiality policies, procedures and protocols as set out in its Privacy Code, that protect against the disclosure of information to people who are not authorized to have that information.

(c) Misuse of Data

(i) _____ (name of Supplier Company) shall institute auditing mechanisms that are used to detect unauthorized access or attempts to access Personal Health Information after they have taken place and monitoring systems so that such unauthorized access or attempts to access Personal Health Information can be recognized while they are occurring.

(ii) In the event that _____ (name of supplier company) becomes aware that a person has obtained access to Personal Health Information other than in accordance with this Agreement or _____ (name of supplier company) has used, disclosed or disposed of the Personal Health Information other than in accordance with the Agreement, _____ (name of supplier company) shall immediately notify the _____ (name of organization) and meet and requirements prescribed by law.

(d) Quality Control of Compliance with Confidentiality Requirements

(i) _____ (name of Supplier Company) shall perform audits and undertake monitoring activities to assist in ensuring that the confidentiality provisions of this Agreement are being followed by its employees.

(ii) The _____ (name of organization) may, upon reasonable notice, assess and review _____ (name of supplier company)'s procedures for receiving and processing Personal

Health Information under this Agreement, for the purposes of ensuring that the confidentiality provisions of this Agreement are being complied with. For these purposes, _____ (name of Supplier Company) shall provide the _____ (name of organization) with reasonable access to the policies, procedures and protocols used for purposes of providing the Services and any documents, which may be relevant.

- (iii) In the event that the _____ (name of organization) makes a formal complaint to _____ (name of supplier company) in respect of its compliance with the confidentiality provisions of this Agreement, _____ (name of supplier company) shall, within 2 Business Days of receipt of the complaint, investigate the matter and provide the _____ (name of organization) with an oral report stating the cause of the deficiency, if any, and the steps taken to prevent a recurrence, if required. Within a further 3 Business Days, _____ (name of supplier company) shall provide the _____ (name of organization) with a written report documenting the complaint, investigation, deficiency, if any, and the steps taken to prevent a recurrence, if required.

Phase IV – Sustaining the Gains

Privacy Check List

The Following Check list was adapted from the “Your Privacy Responsibilities”, A Guide for Business and Organizations, the Office of the Privacy Commissioner of Canada

Template 6.4 a — (Refer to Section 2, Phase IV)

for ready-to-use file go to {[hyperlink](#)}

Privacy Obligations	Yes	No
Personal Information Holdings		
Do you have an inventory of personal information holdings (data collection tools -paper and electronic)?	—	—
Do you know where personal information is held (physical locations and files)?	—	—
Do you know who has access to personal information in and outside your organization?	—	—
Accountability		
Have you named a privacy officer who is responsible for your organization’s overall compliance with the Act?		
Can your staff respond to internal and external privacy questions on behalf of the organization, or do they know who should respond?	—	—
Does your staff know who receives and responds to <ul style="list-style-type: none"> - requests for personal information - requests for correction - complaints from the public 	?	?
Do your clients/residents know whom to contact: <ul style="list-style-type: none"> - for general inquiries regarding their personal information - to request their personal information - to request corrections to their personal information - for complaints 	?	?
Is your privacy officer able to explain the steps and procedures for requesting personal information and filing complaints?	?	?
Has your staff been trained on the 10 Principles?	?	?
Is your staff able to explain the purposes for the collection, use and disclosure of personal information in easy to understand terms?	?	?
Is your staff able to explain to individuals when and how they may withdraw consent and what the consequences are, if any, if there is a withdrawal?	?	?
Information for Clients/Residents		
Do you have documents that explain your personal information practices and procedures to your customers <ul style="list-style-type: none"> - Does this information include how to: - Obtain personal information 	?	?

<ul style="list-style-type: none"> - Correct personal information - Make an inquiry or complaint <p>Does the information describe personal information that is</p> <ul style="list-style-type: none"> - held by the organization and how it is used - Disclosed subsidiaries and other parties 		
Limiting Collection, Use and Disclosure and Retention to Identified Purposes		
Have you identified the purposes for which you are collecting personal information?	?	?
Are these purposes identified at or before the time the information is collected?	?	?
Do you collect only the personal information needed for the identified purposes?	?	?
Do you document the purposes for which personal information is collected?	?	?
Have you developed a timetable for retaining and disposing of personal information?	?	?
Consent		
Does your staff know that an individuals' consent must be obtained before or at the time they collect personal information?	?	?
Does your staff know they must obtain an individual's consent before any new use or disclosure of the information?	?	?
Do you use express consent whenever possible and in all cases where the information is sensitive or the individual would reasonably expect it?	—	—
Is your consent statement worded clearly, so that an individual can understand the purposes of collection, use and disclosure?	—	—
Do you make it clear to customers that they need not provide personal information that is not essential to the purposes of the collection, use or disclosure?	—	—
Third Party Contracts		
Do you use contracts to ensure the protection of personal information transferred to a third party for processing?	—	—
Does the contract limit the third party's use of the information to the purposes necessary to fulfil the contract?	—	—
Does the contract require the third party to refer any requests for access or complaints about the information transferred to you?	—	—
Does the contract specify how and when a third party is to dispose of or return any personal information it receives?	—	—
Safeguards		
Have you reviewed your physical, technological and organizational security measures?	—	—
Do they prevent improper access, modification, use, disclosure and or disposal of personal information?	—	—
Is your personal information protected by security safeguards that are appropriate to the <ul style="list-style-type: none"> - Sensitivity of the information - Scale of distribution 	—	—

	- Method of storage		
	Have you developed a “need-to-know” test to limit access to personal information to what is necessary to perform assigned functions?	—	—
	Has your staff been trained about security practices to protect personal information? For example is staff aware that personal information should not be left displayed on their computer screens or desk tops in their absence?	—	—
	Is your staff aware that they should properly identify individuals and establish their right to access the personal information before disclosing it?	—	—
	Do you have rules about who is permitted to add, change, or delete personal information?	—	—
	Is there a records management system that assigns user accounts, access rights and security authorizations?	—	—
	Do you ensure that no unauthorized parties may dispose of, obtain access to or modify or destroy personal information?	—	—
	Requests for Access to Personal Information	—	—
	Is your staff aware of the time limits the law allows to respond to access requests?	—	—
	Can you retrieve personal information to respond to individual access requests with a minimal disruption to operations?	—	—
	Does your information system facilitate the retrieval and accurate reporting of an individual's personal information, including disclosures to third party organizations?	—	—
	Do you provide personal information to individuals at minimal or no costs?	—	—
	Do you advise requesters of costs, if any, before personal information is retrieved?	—	—
	Do you record an individual's response to being notified of the costs of retrieving personal information?	—	—
	Do you provide personal information in a form that is generally understandable (for example do you explain abbreviations)?	—	—
	Does your organization have procedures for responding to request for personal information in an alternate format (such as Braille or audio tapes)?	—	—
	Handling Complaints	?	?
	Can an individual easily find out how to file a complaint?	?	?
	Do you investigate all complaints received you deal with complaints in a timely manner?	?	?
	Are your customer assistance and other front-line staff able to distinguish between complaints under the law from a general inquiry? If unsure, do they discuss this with the individual?	?	?
	Do you advise the individuals about all avenues available for complaint?	?	?
	Are staff responses to public inquiries requests and complaints reviewed to ensure they are handled fairly, accurately and quickly?	?	?

When a complaint is found to be justified do you take appropriate corrective measures, such as amending your privacy policies and advising staff of the outcomes?	?	?
---	---	---

Template 6. 4 b — (Refer to Section 2, Phase IV)

for ready-to-use file go to {[hyperlink](#)}

Handling Complaints

How should my organization deal with complaints?

Your organization should develop simple and easily accessible complaint procedures. Inform complainants of avenues of recourse. They include your organization's own complaint procedures and those of the Privacy Commissioner of Canada.

Be sure to investigate all complaints received and take appropriate measures to correct information handling practices and policies, if the complaint is found to be justified.

- ?? Record the date a complaint is received and the nature of the complaint (e.g. delays in responding to a request, incomplete or inaccurate responses, or improper collection, use, disclosure or retention).
- ?? Acknowledge receipt of the complaint promptly.
- ?? Contact the individual to clarify the complaint, if necessary.
- ?? Assign the investigation to a person with the skills necessary to conduct it fairly and impartially.
- ?? Give the investigator access to all relevant records, employees or others who handled the personal information or access request.
- ?? Notify individuals of the outcome of investigations clearly and promptly, informing them of any relevant steps taken.
- ?? Correct any inaccurate personal information or modify policies and procedures based on the outcome of complaints.

Sample Brochure

Note: If your organization publishes the enclosed brochure, it may be legally liable if it fails to abide by the privacy protection provisions described in the brochure. Only publish this brochure or other similar communications when you can confirm that your organization is adhering to the privacy provisions you have declared.

The _____ exists to provide you with a broad variety of care and services. To meet your needs and serve you well, the _____ needs to know personal information about you.

You, as an individual, have a right to know how we collect, use and disclose personal information. You have a right to expect that, to the best of our ability, your personal information held by us remains accurate, confidential and secure.

The _____ is proud of its commitment to maintaining the confidentiality and security of personal information and we've provided this write-up to explain how we protect the privacy of individual client's information in our organization(s).

The _____ Privacy Code is based on the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information and the Federal Personal Information Protection and Electronic Documents Act.

It is important that a trust relationship be established between you and our organization. To this end, we are pleased to share information with you. The more you know about us, the more confident you can feel about receiving our services. Similarly, the more we know about you, the better we can serve you.

The _____ collects and uses information about you for only the following purposes:

- ?? To make decisions about the types of services you need
- ?? To serve as a means to communicate with service providers
- ?? To monitor the provision of services and evaluate your response to services provided
- ?? As a legal document made in the normal course of business
- ?? To serve as a record of services provided
- ?? As proof of what was done, by whom and when during a client's/resident's encounter with a provider.
- ?? To be used as evidence against or for the organizations, the service providers or the client.
- ?? To verify our accountability
- ?? For strategic planning, decision making, allocating of resources.
- ?? To meet legal and regulatory requirements

Because it is important that we keep your trust, we will only ask for information which we need and when we ask you for information, we'll let you know why we need it. To the best of our ability, we will seek your consent to verify and supplement information collected from external sources such as Community Care Access Centres, physicians, social services, Ministry of Health and Long-Term-Care.

Subject to legal or contractual requirements, you can refuse to consent to our collection, use or disclosure of information at any time provided the consent does not relate to certain information required for care provisions such as disclosure of information to the Ministry of Health and Long-term-care.

If you refuse or withdraw your consent to the collection, use or disclosure of information about you, we may not be able to continue to provide you with some services that you require.

With your consent and where laws allow this, we may share your personal information with other service providers such as a hospital, pharmacy, medical specialist, social worker; provide services directly to you as required. If you do not want to be contacted by these other service providers, we will withhold information from them.

Under normal circumstance, we won't collect, use or disclose your personal information without your consent. Disclosure means providing specific information about you from our records to a third party.

The only exceptions to this rule are when the disclosure is permitted by law or when it is impossible or impractical to get your consent.

Some examples of situations where we will not seek your consent for disclosure are:

- ?? For emergency or life threatening events
- ?? Where there is legal obligation to disclose under a court or government order, for instance to police
- ?? Where personal information is given to their agents and service providers for services such as laboratory and pharmacy services
- ?? Where personal information must be given to insurers in connection with insurance services

Except as outlined below, a record is kept each time personal information is disclosed, noting the nature of the disclosure, the date and the identity of the party to whom the disclosure was made. Individual records of disclosure are not maintained for regular and routine actions such as prescriptions sent to the pharmacy.

We attempt to ensure that the information we hold about you is accurate, complete and up-to-date. If there are changes to your information, e.g. a new SDM has been named, please notify us immediately.

If you believe that information in your records may be inaccurate, we make it easy for you to access, verify and update it. If information has been provided to third parties, we will convey the corrected information to them if necessary.

If we do not agree to change your personal information, you may challenge our decision. We will make a record of this challenge and, if necessary disclose the challenge to third parties who also process your information.

To review your personal information simply ask a staff person for assistance. The staff person will provide you with instructions about accessing your information. There may be a charge for retrieving your information in which case you will be notified in advance and may if you lie, withdraw your request. You may also challenge the reasonableness of the charge.

Access to information may be more meaningful to you if such access is provided in the presence of a service provider who can explain terminology and the organization's policies. We encourage you to invite a care provider from the centre to assist you in your review of your personal information.

Sometimes a staff person will not provide you with information about you that is within its control. This can occur if your right of access is constrained pursuant to the provisions of PIEPDA.

For example, the staff person will not provide you with personal information if:

- ?? It would reveal personal information about another party and your personal information cannot be separated.
- ?? The information is subject to solicitor-client or litigation privilege
- ?? The information is used for the detection and prevention of a criminal activity and dealings in the proceeds of crime.

If a staff person refuses your request for access to personal information, you will be told why, unless prohibited by law. You may challenge the decision.

Once you have the information, all you have to do is check for its accuracy and let us know if there are any corrections required. We will correct our records or make a note of differences. If information has been provided to third parties, we will convey the corrected information or note any differences to them, if necessary.

Ultimately senior management is responsible for protecting client's information. They delegate day-to-day responsibilities to others, such as privacy officers, within the organization. Every staff person must take responsibility for protecting client privacy, confidentiality and security.

Our suppliers sign contracts that oblige them to contractually adhere to our privacy practices thus protecting the personal information of clients when in the possession of third parties. These suppliers or third parties include lab, pharmacy, physicians, dietitians.

There are controls over the use of computers, paper documents, faxing activities, access to personal information.

If you or your family have concerns or questions about the management of personal information in our organization or about our compliance with privacy codes and laws, we

invite you to direct your questions and concerns to a staff person who is providing service to you. If that person is unable to effectively respond to your questions and concerns, we encourage you to contact our privacy officer at telephone number _____ . We trust that we will be able to resolve any issues that you have regarding the protection of personal information.

If our privacy officer is unable to satisfy your inquiries, you may contact the Office of the Privacy Commissioner of Ontario:

Information and Privacy Commissioner/Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario
M5S 2V1

Tel: 416 326 3333
Toll Free: 1 800 387 0073

OR the

Federal Privacy Commissioner.

Federal Privacy Commissioner
112 Kent Street
Ottawa, Ontario
K1A 1H3

Tel: 613 995 8210
Toll Free: 1 800 282 1376

Section 4 – Frequently Asked Questions

7 a.	Generic Privacy FAQs	85
7 b.	FAQs specific to Long-term-care and Community Care	88
7 c.	FAQs for not-for- profit organizations	95
8.	Bibliography	99

7. a Generic FAQs

Following are commonly asked generic questions pertaining to Privacy practices in general. These are intended to inform organizations, rather than be posted for clients/residents. Web sites may provide additional information on these subjects.

1. What is Personal Health Information?

A. Definition is taken from the Act (PIPEDA Part 1. Definitions). "Personal health information", with respect to an individual, whether living or deceased, means:

- (a) information concerning the physical or mental health of the individual;
- (b) information concerning any health service provided to the individual;
- (c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- (d) information that is collected in the course of providing health services to the individual; or
- (e) information that is collected incidentally to the provision of health services to the individual.

2. Does PIPEDA apply to information collected prior to January 1, 2004?

A. Personal information that your company has collected during the course of its commercial activities is subject to the Act. Since it has already been collected, you don't need to go back and obtain consent to having collected it before the Act came into force. However, in order to continue to use or disclose this information, you now require consent. If you did not have consent in the first place, you will have to obtain it to continue to use the information. For example, some organizations have informed all their customers what they do with their information, to whom it is disclosed and given customers the option to object to these ongoing uses or disclosures. www.privacyforbusiness.ic.gc.ca.

3. How much information should I collect from an individual?

A. The collection of personal information should be limited to the amount and type of the information that is necessary for the identified purposes. Personal information should not be collected indiscriminately. By reducing the amount of information gathered, you can lower the cost of collecting, storing, retaining and ultimately archiving data. Collecting less information also reduces the risk of inappropriate uses and disclosures. www.privacyforbusiness.ic.gc.ca.

4. Who complains to the Privacy Commissioner?

- A.** Complaints are confidential and can come from any source - a competitor, a client or an employee. Individuals will have the right to complain about any aspect of an organization's compliance with the provisions relating to the protection of personal information, and all complaints are investigated. www.privacyforbusiness.ic.gc.ca.

5. Can a resident or substitute decision maker view their chart or have changes made?

- A.** PIPEDA gives individuals the right to access their records and request that errors or omissions in records be corrected.

If residents or substitute decision makers want to review their records or request that health information be corrected, they may do so. The organization has a maximum of 30 days to decide if the request will be granted.

If the organization refuses the request for correction, the resident, SDM may ask for a written statement of disagreement to be attached to their health record. If PIPEDA applies and they are not satisfied with the organization's response, they may request that the Office of the Privacy Commissioner of Canada review the organization's decision.

Taken and modified from <http://www.oipc.ab.ca/hia/DetailsPage.cfm?id=107>

6. What powers does the federal Privacy Commissioner Have?

- A.** The federal Privacy Commissioner is empowered to audit the practices of organizations to ensure compliance with the legislation's requirements. Individual can file complaints for investigation by the Privacy Commissioner, and have the right to apply to the Federal Court for a hearing and remedies which can include an award of damages and punitive damages. Obstructing the Privacy Commissioner's audit or investigation is an offence punishable by a fine of up to \$100,000. "Whistle blowing" provisions protect the anonymity of the employees who report violations to the Privacy Commissioner and prohibit employer retaliation. <http://www.torlys.com/publications/pdf/AR2001-2T.pdf>

7. Does PIPEDA Apply to Employee Information?

- A.** No, PIPEDA will not apply to the employee information of companies subject to provincial labour and employment jurisdiction, unless an employer uses employee information for commercial purposes (as opposed to using it to administer the employment relationship). As a result, employers under provincial jurisdiction will not be subject to privacy legislation unless the province(s) in which the company has employees enacts private-sector privacy legislation applicable to employers.

PIPEDA will not apply to businesses in relation to their employees unless they are federally-regulated entities (for example, banks, transportation and telecommunication and broadcasting companies).

<http://www.osler.com/index.asp?menuid=86&miid=344&layid=124&csid=3033&csid1=1452>

<http://www.osler.com/index.asp?menuid=86&miid=86&layid=124&csid=3032&csid1=1342>

7 b. FAQs for Long-term-care and Community Care

The following FAQs are organized by heading and intended to serve as a guideline for good information practices in long-term-care and community care organizations.

PIPEDA

1. Will there be compliance officers (PIPEDA Police) or is the legislation complaint based?

A. PIPEDA is complaint driven. There are no Privacy compliance officers.

2. Does PIPEDA apply to employee information

A. No. PIPEDA will not apply to employee information, unless the organization is involved in a “federal work, undertaking or business (i.e. Subject to the *Canada Labour Code*). The employee/employer relationship is under provincial jurisdiction and covered labour laws.

PIPEDA would apply if the employer is disclosing (selling) employee information for something outside the employee/employer relationship. However, such activity is prohibited under labour laws.

3. Are there privacy considerations in soliciting employees to become donors?

A. It is good practice to advise employees that their information will be used for this purpose.

4. Municipalities are covered by MFIPPA. What happens if provincial legislation is introduced?

A. If provincial legislation is introduced, the Municipal and District Homes will be subject to it. Provincial legislation will likely be similar to PIPEDA and the CSA Code. Complying with PIPEDA now will help ensure compliance with any new provincial legislation.

5. Will complaints be made provincially first or federally?

A. Complaints are made to the jurisdiction under which the complaint is lodged. If the complaint relates to an organization under PIPEDA, the complaint would be to the Federal privacy commissioner’s office. If the complaint relates to an organization under MFIPPA, the complaint would go to the Office of the Ontario Privacy Commissioner.

Fundraising

6. Is Fundraising considered a Commercial Activity?

- A.** It may be possible to argue that fundraising for charitable purposes may not be commercial in nature. However, because PIPEDA specifically refers to fund raising lists, it is more prudent to assume that fundraising activities are subject to PIPEDA and adhere to privacy principles in the fund raising activity, e.g. obtain consent, limit collection, etc. This will protect your organization from complaints and possible court actions.

7. Can we provide resident lists to our foundation?

- A.** It is good practice to notify and get consent from the individual to disclose their name to the foundation.

Care and Consent

8. Is a general consent ok?

- A.** Yes, so long as the resident has knowledge of what he/she is consenting to. Ideally a Notice would be provided and a verbal explanation given.

9. Assuming a general consent is in place when accessing information from another organization, is consent required?

- A.** The general consent may cover this access; however, the disclosing organization may require a specific written consent before disclosing their records to you.

10. Is it ok to post resident names on notice boards, in sign out books or other places?

- A.** It is advisable that, if names are posted, that this practice be communicated at the time of admission/include it in the admission package. The resident has the right to place restrictions on where their name is posted. The organization should make reasonable efforts to comply with the resident/SDM requests. It may be appropriate to place assignment boards, etc in a place that is not visible to the public but visible to staff and to use initials rather than full names.

11. If a resident's status changes over time and they are not able to make decisions, should a new consent be obtained?

- A.** It is recommended that, if the resident becomes incapable, a SDM should be identified and the consent renewed by the SDM.

- 12. If there is a change in the purposes for collecting personal information, should a new consent be obtained?**
- A.** It is recommended that consent be renewed when there is a change in purpose, use or disclosure of the information collected.
- 13. How do you protect confidential resident information regarding diagnoses (SARS, MRSA, VRE, and AIDS) in a Long-Term-Care Facility?**
- A.** A flag in the computer system may be utilized for those with access to move on to the next screen. The information should not be available to those who do not need access to it. This is more difficult to do in the paper record. If it is required to manage risk, this information may be required in the room or on the door to prevent exposure to others.
- 14. Some family members may not want other family members accessing information about the resident, how does the organization handle this?**
- A.** The organization should follow the wishes of the resident/client/SDM and establish rules to avoid getting caught in the middle. It is better to try to deal with this situation in advance and plan for it, rather than receiving a complaint afterwards. If the resident/client/family's request cannot reasonably be accommodated, they should be so advised and an alternative plan developed.
- 15. How should an organization avoid unnecessary access by staff, families and visitors to personal information?**
- A.** Through the education program and communications, a privacy sensitive culture should be established. Use of initials rather than names when visitors are within hearing range should be encouraged and not discussing residents/clients in elevators, staff lounge, in the corridor, or public areas.
- 16. A CCAC gets information from a resident who is in one facility and applying to another, who gets consent?**
- A.** The CCAC should already have consent from the client to share information with the facilities the individual is applying to. It also behooves the facility to have consent for release of information.

Access to the record

- 17. If families and support staff such as housekeeping are part of the health care team should they have access to the chart?**
- A.** If family and support staff is considered part of the health team, they require education on privacy expectations, confidentiality and clear guidelines on access to personal information. It is unlikely that they require access to the full record.

- 18. When the client record is in the home, how do you prevent unauthorized breaches?**
- A. You can't. You must try to balance the need for continuity of care with privacy concerns. The obligation is on the provider to chart appropriately and document enough information for the next provider. The individual has the right to access the information. You should advise the individual why the information needs to be kept in the house and encourage them to treat it confidentially.
- 19. Should staff be able to access all resident charts (paper or electronic)?**
- A. Staff responsible for providing care and services may have authorized access to the chart (paper or electronic). However staff should only access the information they require to do their job. The organization should have policy in place to this effect and audit routinely for unauthorized access. Confidentiality Agreements should be signed on hire and on a regular basis.
- 20. When a practitioner sees someone they do not know reviewing a chart, what is the correct course of action?**
- A. Staff should be educated to question anyone they are not familiar with who is reviewing charts or accessing personal information. As an organization you should also have reasonable supervision of resident/client personal information and review where it is kept and stored. It may be useful for employees, providers and volunteers to wear badges identifying them as employees or agents of the organization.

Technology

- 21. Is faxing and emailing personal information acceptable?**
- A. Both faxing and emailing can be easily misdirected by faxing to the wrong number or sending to the incorrect email address. Faxing should only be used when:
- ?? when absolutely essential (required urgently),
 - ?? data should be anonymous where possible,
 - ?? a cover sheet that reads "Confidential" should always be attached
 - ?? the receiver notified when it is being sent
- For emailing personal information, include confidential notice in the email and consider encryption and other safeguards.
- 22. Is access to the organization's information system from home allowable and secure enough?**
- A. Yes, remote access to the information system is allowable if it is necessary to the provision of care. The organization needs to be confident that the system is secure enough and policies are in place so that individuals accessing information will ensure information protection and confidentiality. (the information should not be accessed

or available to unauthorized users). Organizational policies should be established to specify which users are authorized to have remote access. Both the organization and the user must be accountable for ensuring data protection at all times. Privacy and security issues should be reviewed with your technology service providers.

23. What safeguards need to be put in place for outsourcing computer technology?

- A.** It is good practice to have contractual language that holds the outsourced company accountable for the protection of any personal information they have access to.

Compliance

24. Can the Ministry of Health and Long-Term-Care access resident information for classification and compliance purposes?

- A.** The Ministry has authority through legislation to access identifiable resident information and has a statutory mandate to undertake a compliance review and has the authority to monitor the care as the funder. Any request for such information should be made in writing. Disclosure should be limited to the purpose for which the compliance advisor requires it and the organization should define the purposes for which their personal health information may be used as part of the notice and consent, including complying with legal and regulatory requirements.

Privacy Review

25. Where can one get help for GAP analysis?

- A.** A complete gap analysis protocol is available at www.privacy.com/privacysource/tools.asp. Local hospitals that have gone through the process may be willing to assist and to share polices.

26. With a multidisciplinary approach to care, all has responsibility for recording some information. How does an organization determine who has access to what?

- A.** As part of the privacy review, categories of information should be established and a determination of what roles in the organization has access to what categories of information. Unregulated workers may not require all of the information. The organization should ensure that they receive the right level of education and information access to do their job.

27. For a small supportive housing operation, what minimum requirements are required for content of the record, consent, record retention and storage and disposal?

- A.** The size of your organization is irrelevant; it is advisable to follow the 10 fair information principles.

Third Parties

28. Can personal information be disclosed to insurance companies?

- A.** Disclosure of resident/client personal information to insurance companies should only be done with consent.

29. What is the facility's obligation for information that was collected by the CCAC?

- A.** It is the CCAC's responsibility to be compliant with the legislation for information they collect, use and disclose. The CCAC must identify its purposes for collection, use and disclosure and comply with these purposes. The Long-term-care facility should advise the CCAC if there is information being disclosed to the facility that it does not require, e.g. there is no purpose for the disclosure.

30. What is the obligation of the organization to notify the resident/SDM of employee on investigations by third parties?

- A.** In the event that a professional college or arbitrator is investigating misconduct or incompetence allegations, they should be asked to identify their authority to receive confidential patient information without patient consent. If they have such authority, the information can be disclosed without consent. Otherwise, they will need to obtain consent. The organization should determine, on a case by case basis, whether the resident/SDM is informed that the record is being reviewed by the arbitrator or college.

31. Several external providers/ suppliers such as pharmacies and incontinent product suppliers have access to personal information- what steps are required for privacy protection?

- A.** Organizations should have third party agreements in place as per the guidelines. Commercial companies will be subject to PIPEDA and should be compliant with the 10 principles

32. What if supplier/contractor refuse to adhere to privacy requirements?

- A.** Outside suppliers/contractors will be subject to PIPEDA whether it is in the contract or not. The onus will be on the supplier/contractor to comply or a complaint can be lodged against them.

Your obligation is to choose your outside suppliers/contractors with care and take reasonable steps to ensure that they protect the privacy of your resident/clients. If they refuse to comply with PIPEDA, this could be a reason to consider not contracting with that supplier in the first place or to not renew the contract.

Retention of Records

33. How long do you keep health records and how do you handle destruction?

- A. Policies for the period of retention of records are required and once the period has elapsed, the organization can destroy the record. The destruction of the record requires a written procedure. The procedure identifies the names of the individuals whose files are destroyed, the date of destruction, the manner of destruction (assurance must be available that the destruction was complete) along with sign-off from an executive officer that destruction has occurred. You must comply with any statutory requirements for the retention of specific records that are applicable to your organization.

7 c. FAQs specific to Not-for-Profit Organizations

- 1. LTCF collect resident co-payment, preferred revenue and funds for non-insured services such as mobility aids, hairdressing and outings is this subject to PIPEDA? Are these activities considered commercial activity?**

- A.** PIPEDA applies to “commercial activities”. To this point, the definition of “commercial activities”, and particularly how that applies in the non-profit health care sector, has not been considered by the courts.

There is accordingly some uncertainty as to the extent to which PIPEDA will apply to OANHSS members, which are non-profit health care or service organizations. As far as the core non-profit activities are concerned, it is generally accepted that PIPEDA will not apply to these activities. However, it may apply to for-profit activities as these are closer to being “commercial”. This issue can be argued both ways, and it will likely be some time before we have any clarification from the courts.

As far as collection of the co-payment is concerned, this is not a for-profit activity, but merely cost recovery as the government funding is not sufficient to meet the costs of caring for the resident.

For the other activities listed above, there are two considerations – is the activity commercial in nature, or is it health care related? Is there a profit, or is it simply on a cost-recovery basis?

Finally, for activities like hairdressing and outings, there is probably not much, if any, personal information that is collected in the course of those activities.

- 2. Is there a clear definition of what constitutes health care activities?**

- A.** There is no definition of “health care activities” in PIPEDA. It only defines “personal health information” (see above), which is a subset of “personal information” generally.

As for a definition of “health care activities”, we would refer to the Ontario Healthcare Consent Act, which deals with consent to health care. That Act sets out the framework for consent to treatment, admission to care facilities and personal assistance services. While “health care activities” is not actually defined in that Act, all of these activities are implicitly characterized as “health care activities” because they are included in that Act. This is a reasonable way to define “health care activities”, as related to the actual treatment of the patient, admission to the facility and personal assistance services that are provided to them.

3. Is supportive housing subject to PIPEDA?

- A.** The answer to this question depends on whether the supportive housing is primarily a health care or other assistive service, or whether it is mainly about providing housing, and further whether it is delivered on a commercial or for-profit basis. The provision of rental housing is certainly typically within the scope of “commercial activity”, so consideration will have to be given to the nature of the services that are provided to the resident and the basis for payment.

4. Are retirement homes subject to PIPEDA? Retirement homes are private pay; the tenant purchases all services (accommodation, meals, laundry services and personal care if required)

- A.** It is difficult to answer this question definitively. The activities of retirement homes, which do not provide health or personal care unless required, are more like commercial activities. However, if they are provided on a strictly non-profit basis, it can certainly be argued that they are not commercial.

5. Are private, non-profit, charitable organizations that provide housing and long-term-care subject to PIPEDA? (they collect resident co-payment)

- A.** If the only payment is the co-payment, then it is not likely that these activities are commercial activities.

Consent and Access

6. Will a global consent on admission covering the collection, use and disclosure to labs, physicians, hospitals, research, fundraising, electronic transmission, fax, etc. be satisfactory?

- A.** Privacy is based on the principle that the individual has a right to know and consent to the collection, use and disclosure of his/her information. Global consent forms are permissible, but only so long as the individual can be said to have “knowledge and consent”. The longer and more complicated that the notice form is, the more likely it is that the individual really does not know what they are being asked to consent to.

As a general principle, we would suggest that general consents or notice forms cover more common uses and disclosures. If there are specific uses and disclosures that are needed only for individual or smaller groups of clients/residents, these should be dealt with on an individual basis (for example, a specific consent would typically be obtained for the disclosure of records to another organization, to facilitate care of the patient on transfer).

7. Can the family member of a deceased resident access the residents chart after death? Does the POA still apply after death for access to records?

- A.** The Power of Attorney is only effective while the resident is alive. After death, it is the person who is in charge of the deceased’s estate that is entitled to access the

deceased's chart. This is typically the executor under the deceased's will or the estate representative appointed by the court if there is no will.

8. Can the lab results from hospital be available to the long-term-care/community care organization after a client has had treatment such as dialysis at the hospital?

- A.** These records can be obtained with the client's consent. Generally, hospitals will require a written consent signed by the client or SDM before they will provide records to you.

Information Systems

9. Many organizations use a web enabled Application service provider for the resident record and billing. What agreements or policies need to be put in place regarding vendor access to the data base? How should the electronic record be archived? Should the organization print the entire record at time of discharge or death?

- A.** Privacy and security issues for computer systems should be reviewed with your technology service providers, to ensure that there is appropriate security on the system. Contracts with all outside suppliers should include confidentiality provisions, which should include that the vendor will only access personal information in the database that is necessary for them to do their job.

For retention and printing of the record, the information must be available and accessible for the applicable statutory retention periods. The record does not necessarily have to be printed, so long as it will remain accessible in digital format. This is something that you should address with your technology service provider.

10. What safeguards are required in using web-based software for the client record?

- A.** Principle 7 of the CSA Code requires that "personal information shall be protected by security safeguards appropriate to the sensitivity of the information". The Code goes on to suggest that higher levels of protection are required for more sensitive information. Personal information in the client record is generally very sensitive, and should therefore be well protected. You should discuss this with your technology service provider, to put in place an appropriate level of security

11. In the course of business, emails from clients/SDMs are often forwarded to others for action, etc. without the consent of the originator? Is this acceptable practice?

- A.** As far as consent to involving others in care issues, this is typically something that the client/SDM has consented to on admission, at least for forwarding within the organization and for care purposes. However, if the disclosure is for other purposes and/or is going to another organization, you should obtain the client's consent.

Other

- 12. Community based groups often come into the facility to entertain, visit, provides education. Are confidentiality agreements required with all of the individuals?**
- A.** If the volunteers from the community group are going to have access to personal information of clients/residents, it would be advisable for them to sign the confidentiality agreement.

8. Bibliography

Borden Ladner Gervais, Patrick Hawkins, Memo November 10 2003

Canadian Standards Association, <http://www.csa.ca/standards/privacy/>

"Guidelines for Managing Privacy, Data Protection and Security" - Ontario Hospital Association (OHA), through the OHA's eHealth Council Privacy and Security Working Group

Information and Privacy Commissioner of Ontario: www.ipc.on.ca

Management Board Secretariat of Ontario has a PIA Methodology/Guidelines: <http://www.gov.on.ca/MBS/english/fip/pia/index.html>

OANHSS Privacy Compliance for the Not-For-Profit Sector Conference, Thursday October 30 2003, Holiday Inn, Toronto

Priva-C: www.priva-c.com/privacysource/tools.asp

Privacy For Business by Industry Canada', www.priva-c.com/privacysource/tools.asp

The Alberta Medical Association provides Guidelines to conduct a PIA in a physicians office: http://www.albertadoctors.org/advocacy/healthinfo/privacy_impact_statements.htm

The Office of the Information and Privacy Commissioner for British Columbia, <http://www.oipc.bc.ca>

Treasury Board of Canada Secretariat has introduced a PIA eLearning tool: http://www.cio-dpi.gc.ca/pgol-pged/index_e.asp

"Your Privacy Responsibilities", A Guide for Business and Organizations, the Office of the Privacy Commissioner of Canada