Document 11:

Harmonizing Research & Privacy: Standards for a Collaborative Future.

Phase III Final Report:

Privacy Best Practices for Secondary Data Use (SDU)

Paulette K Collins, Pamela M Slaughter, Noralou Roos, Karen M Weisbaum, Marie Hirtle, JI (Jack) Williams, Patricia Martens, Andreas Laupacis
Harmonizing Research & Privacy: Standards for a Collaborative Future.

Introduction

The ‘new’ climate and increasing complexity of privacy legislation and heightened concern regarding secondary data use (SDU) for research purposes without consent has important ramifications for the concomitant desire across the country to improve what Canadians report valuing most highly – their Canadian universal health care system. Understanding waiting times, medical error, drug utilization patterns, outcomes of procedures such as bypass surgery and angioplasty, and rationalizing the delivery of primary care (among other issues) – are all critically dependent on the ability to undertake research using data collected in the course of providing health care services. Facilitation of comparative analysis and collaborative epidemiological, health service and policy research (HSPR), statistical and population-based research using these secondary (i.e., administrative, survey, registry and clinical) data by researchers and clinicians across Canada has never been more important to achieve the changes necessary for sustainability well into the 21st century.

HSPR methodologies, often conducted under statutory-based waiver of consent, can be used with population-based health data to provide evidence upon which to base strategic decisions and investments in health, as well as inform clinical practice. Coupled with the need for more research of this genre is an additional call for openness and transparency in how provincial Ministries of Health are using resources to provide good quality care. It is fiscally responsible — some argue a morale responsibility — to employ the data generated by public use of the health care system to evaluate, manage and improve performance of that system.

This unique opportunity requires tools and best practices to help ease and navigate through the complex privacy legislation respectfully and expediently. These tools would also ensure that Canadians do not encounter the same difficulties being reported in other jurisdictions such as the United Kingdom, Australia and the United States.

1 Stanley F. The paradox of progress.- increasing social gradients in health. In the John Chalmers Oration, July 8, 2004 Adelaide, Australia
Over the last six years, in response to provincial and/or federal legislation, some Canadian SDU research organizations have developed privacy codes, confidentiality and research agreement templates, data security policies and access guidelines. These documents constitute policies, practices and procedures pertaining to privacy and data security issues for the secondary use of personal health information found in large administrative and survey databases, both with and without consent. These organizations have also worked with their provincial Privacy Commissioners/ Ombudsman, sharing these documents, obtaining feedback and acting on their suggestions.

Through these processes, these organizations have developed insight into a variety of data issues and have enjoyed mutual benefit in sharing their approaches to privacy policies and procedures. Sharing templates between organizations enabled the successful resolution of several data issues in their home jurisdictions. However, it became apparent that facilitation of comparative analysis and collaborative research among Canadian investigators across Canada required further development of harmonized standards, policies and best practices for the protection of personal health information.

It is also clear that specific knowledge about how privacy issues are handled by SDU organizations and the use of shared practical experiences will facilitate the development of harmonized privacy best practices across these Canadian organizations. This knowledge exchange also has the added benefit to stimulate and encourage ongoing collaborative research activity.

The SDU research community in Canada recognized the utility in considering development of harmonized privacy best practices by agreeing to participate in a series of workshops proposed by the Institute for Clinical Evaluative Sciences (ICES) and the Manitoba Centre for Health Policy (MCHP) (Workshop Phases I & II). For Workshop Phase III planned for 2006, the team was expanded. The workshops initiative was funded by a multi-institute grant from the Canadian Institutes for Health Research (CIHR), under the aegis of the Institute for Health Services and Policy Research (IHSPR), and the Canadian Institute for Health Information (CIHI) Canadian Population Health Initiative (for complete list of funding agencies, see Appendix 1).

The original objective of the workshops was to develop harmonized privacy standards for secondary data use.

There are certain characteristics of SDU research that do not fit the common research model. Defending these differences creates additional work and expense, delaying the launch of legitimate research projects. By articulating these differences clearly, developing an acceptable set of privacy best practices for SDU, being transparent and accountable to

---

5 Institute for Clinical Evaluative Sciences (ICES), Toronto ON, and the Manitoba Centre for Health Policy (MCHP), Winnipeg MB.

6 Joined in 2005 by BC Centre for Health Services & Policy Research (CHSPR) and BC Population Health and Learning Observatory (PHLO); Saskatchewan Health Quality Council (SHQC); Office of the Information and Privacy Commissioner of Ontario (IPC); Queen’s University Department of Family Medicine; Population Health Research Unit (PHRU) at Dalhousie University; Center for Bioethics (IRCM), Montreal.
Canadians for this research done for the ‘common good’, we anticipate that the difficulties with which SDU research currently grapples will dissipate.

The Project

The three phase workshops, entitled Harmonizing Research and Privacy: Standards for a Collaborative Future Phases I - III, included health services and policy researchers, epidemiologists, statisticians, data providers/ stewards/trustees, data custodians and medical record managers, with additional input from the provincial privacy oversight bodies and health law specialists (Appendix 2 – List of Participants).

At the outset of this project in late 2002 to build what became the Privacy Best Practices for SDU, the research team sought to pull together a consensual “standard” of privacy protection. By January 2006, it was apparent that we were articulating and sharing practical and acceptable methods for SDU research – privacy best practices. For some workshop participants, the use of the term “standard” implied fixed criteria (i.e., ISO standards) that are not achievable, given the variation in provincial privacy legislation. For that reason, and acting on feedback from workshop participants and from reviewers across Canada, the decision was made to adopt a more pragmatic approach; specifically, to pursue agreement on a set of privacy best practices to guide SDU research. This approach proved to be extremely fruitful, and from the workshop a set of Tools were developed. These tools will aid organizations and researchers in two ways: 1) in defining privacy-protective performance expectations and, 2) in providing methods for putting practices, policies, procedures and processes in place to produce a level of privacy protection against which actual performance can be measured.

Workshop Phase I (October, 2003) & II (February, 2004)

Over a combined presentation and discussion period of three and one-half days, the Phase I & II workshops produced preliminary recommendations for a privacy best practices standard for organizations or researchers when using health data found in large administrative databases without consent. The recommendations were reached through a number of strategies: by participants’ sharing of their approaches to privacy policies and procedures; roundtable discussions of key issues; and incorporation of the perspectives of two international experts.

The outcomes of Phase I & II included:

a) a final report 7 which stated the eight key suggestions for inclusion in a Voluntary Privacy “Best Practices” Standard, identified four potential uses of a Standard, outlined the possible next steps for developing the Standard, flagged seven

---

additional important issues to consider, and provided seven recommendations to CIHR; and
b) the inaugural collection of a national “privacy toolkit” of privacy/data security practices, policies and procedures from participants’ organizations across Canada.

The workshop participants clearly determined that the voluntary standard must have enough flexibility to be individualized to reflect/represent local legislative and legal (contractual) requirements, as well as the research culture of each jurisdiction in which SDU research is undertaken. It should be:

- practical,
- inexpensive, and
- easy-to-use.

These last three points were of particular importance because of three widely-reported stumbling blocks:

- researchers’ difficulty in understanding the legal language of the statutes;
- lack of personnel with research and privacy expertise (and lack of research privacy programs in which to train staff); and
- lack of dollars for developing / implementing privacy programs.

Since the requirements for data security and privacy protection are in and of themselves very comparable across Canada because of “substantially similar” requirements for provincial/territorial legislation to protect the privacy of personal health information, the steps taken to comply – the practices, policies and procedures under which the data are held and used for research – create a standard in and of themselves. Phase III of the workshop series was poised to reveal how the best practices for SDU could be created.

Phase III Final Workshop – January 2006

The Phase III workshop built on Phases I & II, as well as the extensive work on health research in the September 2005 CIHR Best Practice for Protecting Privacy in Health Research, and with reference to recommendations from the CIHR-commissioned report by Black et al on access to health data in Canada. Importantly, the intent remained to focus on secondary data use for research without consent, in order to proceduralize these legislative standards. The identified goals for Phase III were:

1. Consensus (if possible) on a harmonized Privacy Best Practices for SDU - research which incorporates the secondary use of data without consent. Compliance with these Best Practices will signify due diligence to research ethics boards (REBs), privacy

---

oversight (commissioners/ombudsman), university research bodies, and other interested agencies/individuals (potentially including granting agencies);

2. Produce a complementary document - specifically geared for research which incorporates the secondary use of data without consent for the CIHR Best Practices for Protecting Privacy in Health Research, September 2005 document.

3. Pilot the Privacy Best Practices for SPU with HSPR researchers and data institutes.

Preparing for January 2006, Phase III

Expansion of the Team
To ensure comprehensive input and facilitate buy-in for the development of best practices, the core members (ICES & MCHP) approached other SDU organizations in early 2005 to participate as co-investigators in the Phase III Workshop. These investigators and their centres augmented the core group, creating a nationally-representative team of research institutes.

Steering Committee
A Steering Committee was struck whose purpose was to review and provide feedback to the research team on the draft documents being developed for the workshop. These documents – the initial framework of the best practices – would serve as a starting point for discussion at the January 2006 workshop (see Appendix 3 for a list of Steering Committee members).

The Steering Committee met twice via teleconference call prior to the January 2006 Workshop. The first call in mid-October reviewed and updated the voluntary standards that were reported in the final workshop summary report – May 2004. The Committee was provided with initial drafts of the evolving reference materials – the legislative scan and “Rules-in-a-Box” documents for discussion and comment for the second conference call, which took place in mid-November. Additional details of these teleconferences can be found in Appendix 4, the main outcomes included:

- Agreement that the structure of the developing framework follow the CIHR Best Practices for Protecting Privacy in Health Research, September 2005 document element-by-element to facilitate usability between the documents.
- The legal analysts had found tremendous differences in interpretation/definitions, validating the plan from Workshops I & II to create a Table of Equivalencies.
- Agreed that the plan to conduct an email survey of a sample of research organizations throughout Canada who conduct SPU to validate the legislative acts that are routinely used would ensure the outcome is meeting requirements.
- The Steering Committee provided the following updates to the May 2004 voluntary privacy standard for SPU:
  - Add an initial threat risk assessment (TRA) / penetration assessment (in some form) - as a basis line and then periodically. TRA could be comforting for custodians as well as research colleagues. Should not be the size of the organization but the sensitivity of the data held that puts this into play.
  - Need a separate piece on data security and safeguards: physical data protection / intrusion detection / electronic safeguards.
Add clarity to the privacy impact assessment: one should be project-specific and one should be organizational-/system-specific. Project-specific privacy review and PIA = systems or database privacy assessment.

Add clarity to the Research agreement. Develop standard templates for data and researcher agreements.

Add clarity to the transparency requirement and define the roles of custodian, user / researcher and provider / stewards.

Define the difference between ‘access’ and ‘disclosure’.

Plain, useable language was an imperative. While it was acknowledged that this will be challenging as the document is based on legal language, efforts will be made to keep the language simple, the documents user-friendly and restrict the legal language to the Statute-by-Statute Analysis document.

The focus of the document is to be a useful, workable document that facilitates the transfer of knowledge in the most effective way.

The objective of the legal scan has been establishing what the minimal standards might be; legislative change is not being sought – this is intended as a policy document.

The importance of establishing these standards was reaffirmed. There needs to be a baseline/foundation that everyone starts with, some minimal best practices that everyone who works with secondary data without consent utilizes.

To create best practices, everyone must start from the same terms of reference. In order to start at this point, the Table of Definitions and Equivalent Terms has been developed.

Discussion about the abundant opportunity for knowledge transfer, how to communicate information to data stewards and data centers and, perhaps most importantly, how to educate the public and the community.

Interest expressed in developing a SDU specific Research Ethics Board (REB). It was felt that this would ensure that the REB was familiar with the rules and regulations of SDU without consent and inform data owners.

**Drafting the Framework**

The development of what has become the Workshop Tools started with the construction of the Reference Materials. The first task for the core research group was to:

a) establish the legislative Acts that SDU organizations routinely use to ensure their work meets legislative requirements in day-to-day operations; and

b) ensure that the underlying premise they were working from – privacy legislation is the foundation from which all jurisdictions work regarding policies and procedures for SDU research – was correct.

To complete this task, two members of the core research group, both legally-trained experts (one with additional training in research ethics) well-known to the SDU community, conducted a brief email survey of established SDU organizations that hold relevant administrative data.
Seventeen organizations (potential Phase III participants) across Canada were asked the question in an email survey: “Assuming privacy legislation is the foundation from which all jurisdictions work, in your institute’s research operations what are the legislative Acts that you routinely use to ensure your work is meeting legislative requirements?” The results indicated that the underlying premise was correct (see Email Survey - Appendix 5).

Then, the common characteristics of SDU organizations were identified. SDU organizations are either:

- governed by statute,
- house and/or manage large administrative databases on behalf of other organizations that are governed by statute, and
- receive and use personal health information for research purposes under a contractual agreement rooted in a statutory obligation.

Next, specific characteristics of SDU research were identified:

- By definition, this type of research is research for which consent is not practical because it uses personal information from the entire population, meeting the test of impracticability.
- This type of research makes use of databases that contain information, including personal information, personal health information, or both, at an individual, linkable level.
- The benefits of this type of research is only accrued when 100% of the data is available and used for the research, making the results generalizable to the population and potentiating the portability of the findings for “the common good”, both nationally and internationally.
- The purposes of collection from the databases for this type of research is secondary to the original purposes of collection. Collection is also indirect; it is collected from custodians of these databases, not directly from individuals. Originally, the information was collected for a different, primary purpose (e.g., physician service claims, drug benefit claims/plans, hospitalization abstracts).
- This type of research is generally population-based. It invariably uses data from large numbers of individuals with whom the researcher has no direct relationship. The data consist of selected elements rather than complete records of personal information and rarely include direct personal identifiers. If data are received with identifiers, these are stripped or encrypted before data is used for research.
- The potential benefits of SDU research and the derived public good must clearly outweigh the potential risk to the privacy of individuals.

It is these common and specific characteristics that guided the structure, content and analysis of the legislative review. The legal analysts reviewed provincial/territorial and federal privacy legislation to identify the “foundational” statutory rules for privacy in SDU across Canada that apply to the handling of identifiable personal/personal health information specific to SDU characteristics. The interpretations of the legislation are intentionally narrow and of specific application to SDU entities that are covered by key statutes.
The statutes are essential to understanding the “foundational” rules for these SDU research organizations and establishing sound policy principles. The rules set standards that, at the very least, must be met by these organizations in order to comply with statutory privacy requirements for collection, use and disclosure of personal information. The requirements apply to all aspects of information handling, including uses and disclosures made for the purpose of research conducted without consent and where waiver of consent is justified.

The “Tables of Concordance with Privacy Legislation” contained of the CIHR Best Practices for Protecting Privacy in Health Research, September 2005 were also reviewed.

The legal analysts proceeded to develop SDU-specific documents that describe the implications of the current legislative landscape vis-à-vis privacy best practices for SDU.

Three purposes were defined for the developing reference materials:

- to define implications for a harmonized privacy best practices for SDU;
- to educate workshop attendees about the legal foundation for privacy best practices for SDU at the January 2006 workshop; and
- to serve as a stand-alone educational document to be released at the same time as the Privacy Best Practices for SDU.

Reference Materials Resulting from the Analysis:

The Encyclopedia: Statute-by-Statute Analysis of Privacy Legislation Relevant to SDU by Jurisdiction

The Statute-by-Statute Analysis of Privacy Legislation Relevant to SDU without consent by Jurisdiction was planned to be structurally similar to the September 2005 CIHR Best Practices for Protecting Privacy in Health Research compendium, allowing for comparison with the CIHR document.

The legal analysts worked from the premise that for SDU research, consent is neither practical nor feasible. If there are circumstances in the research proposal where consent may be practical, that study will fall outside this framework.

A statute-by-statute review of key legislated privacy statutes from across Canada was conducted according to a template with headings that correspond to the Elements in the CIHR Best Practices for Protecting Privacy in Health Research, September 2005. Key legislation includes statutes that are specific to or include applications to health information. It does not include other privacy statutes, such as PIPEDA and some freedom of information statutes. Analysis of these other statutes were incorporated into post-workshop documents.

The statutes were reviewed for the very specific purpose of asking the question “when it comes to SDU research, how is this type of research conducted?” Being able to specifically center the analysis on this question actually optimized the retrievable information for analytic purposes because of the narrow focus of the project. Once completed, the analysis of
individual statutes was shared with privacy commissioners/ombudsman offices for purposes of discussion/verification.

This document provides a readable (lacks legal jargon) interpretation of legislation and regulations for SDU organizations and researchers. As much as possible, this document is specific to organizations that conduct SDU and that are governed by statute. When reading these statutes, the reader must keep in mind their prime goal: protecting the health information of individuals.

**The Translation Document**

This document contains the same material as in the statute-by-statute analysis, but it is organized according to the categories/Elements in the CIHR Best Practices for Protecting Privacy in Health Research, September 2005.

- The left-hand column lists the relevant legal provisions for each province/territory.
- The right-hand column provides non-legal language points – “translating” and distilling – the analysis of what the law requires across Canada’s provinces and territories to protect the privacy of individuals whose health information is used in SDU research – into concise policy rules.

**Dictionary: Table of Definitions and Equivalent Terms**

In this document, ten frequently-used concepts have been identified and the corresponding terms/definitions provided. This provides readers with a basis for finding and comparing terms across statutes. Workshops 1 & 2 taught us that although SDU organizations essentially have the same obligations and practices, language varies widely. The table of equivalencies helps demonstrate the comparability and similarity of obligations (rather than dissimilarities) across jurisdictions.

**Use of the Reference Materials**

In order to make appropriate use of the reference materials, it is essential that readers understand the nature of the analyses.

It is important to understand whether research is a “use” or an activity that follows a “disclosure” of information:

- “Use”: sharing of data by an SDU organization with affiliated researchers
- “Disclosure”: sharing of data by an SDU organization out-of-house with external researchers

USE is specifically the research application of data within the control of a single entity – a standard common to all of the health information laws. DISCLOSURE infers data leaving the control of an entity, from which the data is alienated – it has “lost control” over the information, which now rests in the hands of the designated researcher.
Harmonizing Research & Privacy: Standards for a Collaborative Future.
Privacy Best Practices for Secondary Data Use (SDU)

If the entity retains custody and control of the data, the researcher is working within a **secured environment** – using the data (i.e. Manitoba Centre for Health Policy [MCHP]). If the researcher has both custody and control of a dataset, for purposes of these Tools the researcher is working within an **unsecured environment** – the data were disclosed (i.e. a researcher obtaining a data set from Centre for Health Services and Policy Research [CHSPR]).

The reference materials include references to particular sections, subsections and paragraphs in the statutes from which the analysis is made.

- Some statutory sections have explicit application to SDU organizations. For example, a section may provide an explicit rule for SDU entities that are governed by the Act, such as “only disclose personal information for research where a Research Ethics Board (REB) has approved the plan for safeguarding information.” These organizations may commonly be called repositories, institutes, data custodians, etc – but what is most important in determining whether these explicit statutory rules apply is whether an organization is governed by the legislation. In the **Table of Definitions and Equivalent Terms**, the terms that are used in each statute to refer to the SDU organizations are listed under the category “Covered Entities” in Table Definition 1.
- Other statutory sections apply implicitly to researchers that conduct SDU. For example, the explicit rule — “only disclose personal information for research where an REB has approved the plan for safeguarding information” — is also an implicit rule that researchers must follow — “be sure to provide the REB with sufficient details about how personal information will be safeguarded during the research project.” The explicit statutory rule applies directly to the public body — a necessary condition for disclosure is approval of safeguards. The implicit rule applies to researchers — have a plan for safeguarding information that the REB will approve.

**Development of the Privacy Best Practices for Secondary Data Use (SDU)**

*The Privacy Best Practices for SDU* uses the policy rules from the Translation Document as the foundational requirements for the *Privacy Best Practices for SDU*. Using these rules as a “foundation” does not mean that the best practices needs to be held to this level—the research community can raise or exceed the best practice as it sees fit.

In order to proceduralize the best practice – to “give life” to the policy rules – *The Privacy Best Practices for SDU* cross-references these policy rules to applicable documents - policies, practices and procedures currently used and provided by SDU institutes and centres across Canada. These documents, offered as templates by active researchers for others to use, are found in the Privacy Toolkit for SDU and its companion templates.

*The Privacy Toolkit for SDU + Companion Templates* contains a variety of templates for privacy policies, practices, procedures, confidentiality pledges, security standards, data-sharing agreements, and so on. The items are listed in the toolkit document (for both secured and non-secured environments) and include templates found on the CD. These templates (tools) are meant to be used to proceduralize the best practice and provide users with methods for actions that will meet the requirements of the legislation. Researchers are invited
to borrow liberally from these templates, or use them as a platform to develop their own policies, practices and procedures specific to their own jurisdictions and research cultures. The contributors ask simply that the originating organization be acknowledged in any document created from a template, or, if using the template.

A Privacy Checklist was also developed to facilitate the piloting of the Best Practices. The Checklist provides a process to monitor and facilitate the application and use (as outlined in the Elements) of the Privacy Best Practices for SDU. It facilitates the users’ creation or updating of required policies and procedures as well as producing an inventory to verify that the requirements of the Privacy Best Practices for SDU have been met – or are not applicable.

### Key Message

<table>
<thead>
<tr>
<th>What The Privacy for Best Practices for SDU IS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- It is a translational document, condensing, getting to the bottom line moving from legislation to policy – creating the privacy best practice;</td>
</tr>
<tr>
<td>- This document articulates, validates and intentionizes the policy rules in plain language, cross-referencing the rules to items in the Privacy Toolkit to proceduralize the best practice;</td>
</tr>
<tr>
<td>- It speaks to the possibility of harmonization, and where harmonization is impossible;</td>
</tr>
<tr>
<td>- It is a tool for due diligence, especially where there is consensus from the research community. In terms of due diligence, this document brings us full circle. Having done this exercise, asked the questions and documented the results is, in itself, an exercise in due diligence.</td>
</tr>
<tr>
<td>- It is a useful reference tool, but it’s not the only reference tool.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What The Privacy for Best Practices for SDU IS NOT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- A legal opinion. If you have a legal dilemma, a specific legal issue or question, you need a legal opinion. Providing a professional legal opinion will involve looking not only at obviously relevant legislation and less obviously relevant legislation and case law, but also findings or reports of privacy commissioners and ombudsmen in this particular area;</td>
</tr>
<tr>
<td>- A compliance tool. There is in Manitoba, for example, a very excellent privacy compliance tool that is a check list one can go through to ensure that the minimal requirements of your legislation are being met;</td>
</tr>
<tr>
<td>- A substitute for the statutes; and</td>
</tr>
<tr>
<td>- A static document. It needs to be updated as legislation and regulations change.</td>
</tr>
</tbody>
</table>

### The Phase III Workshop

The workshop was held over a two-day period at the Inn at the Forks on January 16 & 17, 2006 in Winnipeg, Manitoba. The participant group was comprised of 55 diverse individuals from across Canada, including oversight bodies, directors and staff from SDU organizations, researchers, organizational privacy officers, research ethics board members and a member of the public. A professional facilitator ensured that the objectives of the meeting would be met. The facilitator also instituted a “parked notes” board for participants to leave written
comments or notification of concerns at the close of a particular session or element to allow the agenda to move forward.

**DAY ONE**

Morning presentations laid the groundwork for the workshop and provided an overview of pertinent new materials, such as the CIHR Best Practices compendium, released four months earlier. See Appendix 6 – Phase III Workshop Agenda.

The legal analysts walked the participants through the process used to develop the Workshop Tools in preparation for extensive review by the workshop of *The Bottom Line – Privacy Best Practices for SDU*.

**Important Issues Raised From the Process and Overview**

- Some of the participants expressed concern that HSPR also included consent-based research and found it confusing that the documents were labeled HSPR. The suggestion was made to develop another label, even though it was explained in these documents that HSPR referred to statistical/epidemiological/population-based/health services and policy research methodologies that use population-based health data (administrative, survey, registry and clinical) *without consent*. The group was not able to suggest another label, but these types of discussions characterize the confusion that researchers feel in many jurisdictions. To address this issue, the core workshop research team adopted “secondary data use (SDU) organizations”.

- Participants suggested that it was important to have explicit criteria for obtaining waiver of consent, suggesting that these might provide additional guidance to REBs. Clarification of use without consent and consideration of what research methodology would characterize projects that could obtain approval for use without consent was sought, with the suggestion that this information would be valuable for REBs as well. Participants were informed that in terms of legislative standards, there are other bodies that are recognized where REBs are not, who make these decisions and provide approval for research projects to use secondary data *without consent*.

- Participants agreed that the issue of consent is outside the focus of this workshop.

- SDU organizations also use the data entrusted to them for approved research, as allowed in their agreements with the data providers and authorized in legislation, but the roles of Researcher and Trustee can become a bit blurred. The group requested a break down of roles and responsibilities to avoid gaps and redundancy. Participants suggested the development of a schematic diagram to help researchers confirm whether or not the Privacy Best Practices is appropriate to inform them about privacy protections, data security and accountability in a planned research project. See Appendix 7 – Decision Tree

- The participants defined a standard as “a desired and achievable level of performance against which actual performance can be compared”.
Review and Discussion of Elements in *The Bottom Line* - Privacy Best Practices for SDU Document: Issues & Suggestions

**Element 1: General purposes, determining research objectives, justifying the need**

In most of the legislation, there are specific provisions articulating that the legislation doesn’t apply to statistical information or non-identifiable information, and as such, research using these data would be outside of the legislation. In the CIHR Best Practices document, any information which either directly/indirectly (through either linkage to other information or manipulation of the data) could make it possible to identify individuals (i.e., sub-group analyses in SARVs [area variation analysis]). In SDU research, even though the information has been de-identified, the amount and breath of linked data that the researcher is using and analyzing raises the bar, making it worthwhile to consider treating the data *as if it were identifiable*.

There was discussion around the terms ‘sensitive information’ and ‘vulnerable populations’, and reasons that higher standards may/may not be required.

The public health interest should substantially outweigh the public risk-to-privacy interest. Participants felt that the burden of proof lies with the researcher for linkage studies being in the public interest. The assessment of that demonstration of proof should be done by an external body, whether it be a REB, a custodian or some other public body.

**Element 2: Limiting collection**

Researchers are often required to justify the use of each variable they require for their research project to the data custodian.

Participants were confused about ‘who’ was actually doing the collecting: researchers or custodians? Much of discussion of these issues stems from the way language is used by different groups and in the statutes. Technically, if data is de-identified and used for secondary purposes, a researcher would not be ‘collecting’ data (in the usually-understood meaning of collection of health information directly from the individual, with consent). As collection and use are sometimes used interchangeably, it was suggested to review Element 8 next and then return to Element 3 (as below).

**Element 8: Limits on use and disclosure**

Concern was expressed regarding the distinction between the standards which would apply to research data repositories, compared with individual research projects.

Since there are two divergent audiences and the use of the terms ‘collection’ and ‘use’ vary for those two audiences, a suggestion was made to partition the effected elements by who the user of the standard will be – Trustee/Repository or Researcher/Project. SDU data custodians are like ‘gate-keepers’. They are not necessarily the original custodians nor original collectors of the data, but are ‘holding data’ for research use.
Element 3: Determining if consent is required
The workshop participants decided that this element is not really ‘determining’ if consent is necessary. It is the legal premise for research without consent which should be put right at the beginning as this is the type of research we’re talking about. They suggested that this element include where the statutes are that you can refer back to know under what conditions this type of research is allowed.

Element 4, 5, 6: The workshop participants determined that these elements are - Not Applicable to SDU research

Element 7: Safeguarding personal data
Discussion regarding the infrastructure required to store, secure and manage health information, and the possibility of independent oversight to assess the types of safeguards in place suggested an annual/bi-annual auditing mechanism on the physical and structural checks and balances in place within organizations.

The researcher’s responsibilities were clearly spelled out; data steward’s responsibilities need additional clarity. It was also suggested that the responsibilities of repositories versus researchers should be split.

There should be paper as well as electronic safeguards, as it appears that most breaches are via paper.

Element 9: Setting reasonable limits on retention
There appears to be an inherent tension in this element between destroying information once the project is finished, and conserving it for other investigators to confirm recorded results. If the information is destroyed, the trail that could be used to document, validate the research findings or be replicated by others, is destroyed. Time requirements for review processes related to peer review publications must be considered.

An alternative might be to develop infrastructure where a third party archives this information, which would only be accessible for re-examination through a new REB approval. This infrastructure could be within the researcher’s institution, but could also be a centralized repository or a national archive10. In terms of managing the amount and sensitivity of the information, this suggestion offers a practical solution. Additionally, the (SAS) code could be retained and archived by the researcher, while the (linked) dataset could be deleted or stored by third parties. Again, it was felt that there needed to be additional clarity of the rules required for repositories and researcher.

Element 10: Ensuring Accountability and Transparency
As a robust demonstration of transparency, the suggestion was made to provide institutional Privacy Impact Assessments (PIA) to oversight bodies, inviting comments. Registries of

---

disclosures for research purposes should be kept where feasible. A presentation on Day 2 would further inform the discussion of this element.

**DAY TWO**

**Dr. Debra Grant: Office of the Information and Privacy Commissioner of Ontario**

A perspective on responsibilities for Trustees/Custodians was represented, including an initial check list of all the privacy safeguards that should be in place as part of a good privacy program. Organizations, although not expected to have everything on the check list in place, were expected to have a reasonable combination of safeguards. The assessment of ‘reasonableness’ should be related to the nature of the work undertaken by the organization, the level of sensitivity of the information in their custody, the nature and the number of people who have access to personal health information and the controls in place. Generally, privacy programs are categorized by policies, procedures and practices specific to administrative (human resource), security (physical and technological) and privacy safeguards.

Researcher’s responsibilities for the use of personal health information include written applications to the custodian and a detailed REB-approved research plan. External researchers must sign research agreements with the custodian. Researchers are required to comply with any conditions imposed by the REB and are only permitted to use the information for the purposes set out in the research. In the regulation to the Ontario legislation, a series of twelve items must be addressed\(^\text{11}\). In Ontario, REBs have to consider whether the objectives of the research can be accomplished without the use of personal health information; whether the data is going to be adequately protected during the conduct of the research; whether the public interest in privacy overrides the public good of the research; and whether or not obtaining consent would be impractical.

**Element 10: Ensuring Accountability and Transparency, revisited**

Research conducted by a SDU organization that also houses data is often being done under contract – research agreements – between the data provider and the SDU organization. These contracts often spell out all the requirements and obligations for the organization’s use of the data. Policies and procedures should include requirements for informing the public about uses and disclosures of information for research, and the communication of research outcomes. Maintaining technological, administrative and physical safeguards, orientation and training for staff, and requirements of staff confidentiality agreements are all part of public accountability.

Participants noted that research agreements between ‘covered entities’ disclosing personal health information and the researchers who receive the information must outline obligations and requirements to follow the ‘entities’ privacy policies and procedures as appropriate. The

\(^{11}\) Regulation to Ontario’s PHIPA (Reg. 329/04) Section 16. (source: http://www.e-laws.gov.on.ca/DBLaws/Regs/English/040329_e.htm accessed 24 March 2006). Personal Health Information Protection Act (PHIPA) may be found at http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm (accessed 24 March 2006)
same responsibilities that accrue to SDU in-house research for entities should be applied for research done outside that environment, as a general rule. Participants discussed sanctions for breaches of privacy, and suggested using data for purposes other than those agreed upon should be considered a breach. There is a difference between accidental and willful breach.

### Review of Parked Notes

When discussions were completed on the ten elements, the group turned their attention to a review of the Parked Notes Board, where concerns were posted when time ran out in a scheduled discussion period. Following is a summary of those notes.

- Need definitions for covered entities, databases and registries
- Clarification was requested about research plans, research protocols, research submissions, and research agreements and how to differentiate between those things – some of these were addressed in the previous discussions, others will be addressed through the Privacy Toolkit.
- Request was made to harmonize definitions with the CIHR best practices definition where possible. This will be done in the **Table of Definitions and Equivalencies**.
- Ensuring the accuracy of data and requesting a minimum amount of data for research projects; given that researchers are working with imperfect secondary data, they may need to look more broadly in the data to actually construct an accurate measurement.
- It may be reasonably assumed that **data validity work** is an important obligation of both custodians and researchers; the data elements that one needs to request for that work are a legitimate requirement for doing accurate and valid work.
- A higher standard should be in place for research conducted using personal level information **without consent** of the individual.

### Updating the Privacy Toolkit

The participants were asked to provide copies of their privacy documents – administrative, technical and security privacy policies, procedures, practices and processes – for inclusion in the updated Toolkit. The Toolkit that was constructed after Phase II was presented to this group as a baseline for their information and discussion.

The participants again highlighted that voluntary privacy standards (best practices) will not work unless they are simple, practical and unambiguous – and portable to all jurisdictions.

The use of Aboriginal data that involves aggregation of Aboriginal groups has different parameters. It is important to recognize and respect **collective privacy interests** of Aboriginal Nations as appropriate and that research in which data specific to or aggregated for an Aboriginal group or groups requires either prior consultation or requires approval by representatives of that group. Tools developed by NAHO have been included in the Privacy Toolkit since its first iteration in 2004; updated materials have been submitted for inclusion.

### Key Message

“These will be useful documents if we can hand them out to someone new to this field and clearly say, ’These are the principles and practices by which you conduct health services and policy research. These are the kinds of issues you need to address and go through, and this is your starting point, but in addition to that we’ve harmonized our practice across...”
Pulling It All Together

A goal of mid-April 2006 was set for completion of the review and revision of the Workshop Tools. This included assimilating all the discussion information and incorporating the suggestions/edits received at the Phase III Workshop, as well as incorporating additional suggestions and comments from another review by the provincial oversight bodies. These updated Tools were then sent to the entire collaborative research team for final review. After incorporating the final review comments and suggestions, the Tools were sent to a number of collaborators and SDU agencies who volunteered to pilot the Workshop Tools.

We know that privacy and data security requirements will vary depending on jurisdiction and local research culture. As such, the conditions under which the Tools are being piloted/tested must test these different needs. For that reason, "free-form" reporting on whether the Tools were useful, failed to help, or need more adjustment or tweaking provided one method for evaluation and feedback for the Piloting process.

To assist the piloting process of the Privacy Best Practices for SDU, the research team also developed a CHECKLIST. The Checklist can be used as an alternative to, or in conjunction with, “free-form” reporting. The Checklist provides a process to monitor and facilitate the application and use (as outlined in the Elements) of the Privacy Best Practices for SDU. It facilitates the users’ creation or updating of required policies and procedures as well as producing an inventory to verify that the requirements of the Privacy Best Practices for SDU have been met — or, are not applicable.

Some additional benefits of using the Checklist:

- brings together in a single source organizations’ shareable policies and procedures for privacy, confidentiality and security;
- provides privacy, confidentiality and security education, as the process can require consultation with many (or even all) individuals within an organization — particularly if has all team members have an opportunity to review the completed Checklist;
- the completed Checklist can be used to promote communication, openness and transparency, and document due diligence for university research and privacy oversight bodies.

Once the pilot was completed and final changes made, the finalized Workshop Tools and the final report was sent to the workshop participants and CIHI-IHSPR (Summary of Workshop Tools – Appendix 8).
The Resulting Workshop Tools are:

I. PRIVACY BEST PRACTICES FOR SECONDARY DATA USE (SDU)

This document provides the foundation for ensuring respectful SDU. It lays out, in plain language on the left-hand side of the page, a distillation of legislative requirements across Canada’s provinces and territories to protect the privacy of individuals whose health information is used for SDU research. The right-hand column contains titles of templates for policies, practices and procedures contained in the Privacy Toolkit. This document is founded on the Reference materials below – the Translation document originates from the Encyclopedia - Statutes-by-Statutes Analysis.

a) The Privacy Toolkit for SDU (secured and non-secured environments) & Templates

The items in the toolkit provide users with a range of appropriate options - methods for actions that will meet the legislative requirements. These documents are offered as templates (see Appendix 9), by active researchers, for others to use. You are invited to borrow liberally from these, or use them as a platform to develop your own policies, practices and procedures. Organizations and researchers are encouraged to create and tailor a practical application of the Privacy Best Practices for SDU that is appropriate to their local research culture and legislative requirements. You are asked to acknowledge the originating organization in any document created from or if using a template.

b) Checklist for Privacy Best Practices for SDU

The Checklist enables SDU organizations and/or researchers to create and record an inventory of their SDU privacy best practices, by prompting the formalization in written form of all necessary policies and procedures. For those who want to apply the Best Practices for SDU, it's a method to record/monitor/facilitate the application and use of the Best Practices and can help construct the 'big picture' for your organization or project.

II. REFERENCE MATERIALS

a) Encyclopedia - Statute-by-Statute Analysis of Privacy Legislation Relevant to Secondary Data Use Organizations by Jurisdiction - an analysis

This document contains an analysis of the relevant provisions of each key statute by province/territory and provides a readable interpretation of legislation and regulations specific to SDU. Each analysis follows the same categories (Elements) as the CIHR Best Practices for Protecting Privacy in Health Research, September 2005 document, allowing for comparison between the documents.

PI (Personal Information) and PHI (Personal Health Information) are acronyms used throughout the analysis. Not all statutes use the same terms or discriminate between personal information and personal health information. The language used reflects that found in the statutes.
b) The Translation Document

This document contains the same material as in the statute-by-statute analysis, but it is
organized according to the categories/elements in the CIHR Best Practices for Protecting
Privacy in Health Research, September 2005 document. Analysis of the relevant statutory
provisions for each province/territory are in the left-hand column, while the right-hand
column provides non-legal language points – translating and distilling the analysis into
concise policy requirements. These policy requirements form the basis of Privacy Best
Practices for SDU

c) The Dictionary - Table of Definitions and Equivalent Terms

This document contains the ten frequently-used concepts that have been identified and the
 corresponding terms/definitions from each jurisdiction. This provides readers with a basis for
finding and comparing terms across statutes and helps demonstrate the comparability and
similarity of obligations (rather than dissimilarities) across jurisdictions.

Benefits to Stakeholders using the Privacy Best Practices for SDU:

- Organizations and researchers using the Privacy Best Practices for SDU – with the
template provisions for data security and privacy protections, including balancing of
risk and benefit, transparency of purpose, use, retention and accountability, both in
local jurisdictions and in collaborative provincial and national frameworks—would
be assured that they are meeting the legislative requirements that exist.
- These best practices provide a strong foundation for ensuring respectful use of
administrative data for research purposes, a goal that is important to researchers and
the public.
- The Privacy Best Practices for SDU have been reviewed and are acceptable to some
provincial Privacy Commissioners and Ombudsmen, data stewards, and Research
Ethics Boards. Such organizations and their researchers could also potentially be
"pre-certified" for submissions to granting agency competitions for funding.
- The set of best practices provide an authoritative source that has rigorously reviewed
privacy in SDU against the background of PIPEDA’s Ten Guiding Principles and
could be useful in any sort of court challenge regarding SDU.
- The templates in the Toolkit are currently in use by organizations and researchers
engaged in this type of research; thus reduces the need to “start from scratch” and
reduces costs (in and of itself a harmonizing activity). Given concerns of researchers
that privacy expertise is a scarce resource in Canada (and costly to organizations and
researchers already working with tight budgets), this is a practical approach that has
already worked for several of the organizations who undertook this project.
- Provides an accountability standard for the public whose data are used for these
research purposes.
- Provides a tool for due diligence; demonstrates familiarity with legislative
requirements.
Harmonizing Research & Privacy: Standards for a Collaborative Future.
Privacy Best Practices for Secondary Data Use (SDU)

- Provides a checklist for REBs to assess that adequate safeguards are in place to protect the privacy of the individual, and provides REB accountability parameters for the public for its decisions.
- Facilitates review and audit by privacy oversight bodies (generally Privacy Commissioners and Ombudsmen but can be others).
- Can provide an arbitration mechanism when research and privacy are at odds.

<table>
<thead>
<tr>
<th>The Differences Between the CIHR Best Practices for Protecting Privacy in Health Research, September 2005 and the Privacy Best Practices for SDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Privacy Best Practices for SDU differs from the CIHR Best Practices for Protecting Privacy in Health Research, September 2005 in the following ways:</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>The CIHR Best Practices compendium lists all references from each statute that pertain to the topic addressed by a particular Element. For example, any sections in a statute related to consent are listed under the Element(s) that focus on consent. SDU research is research for which consent is not practical; therefore, the SDU-specific scan focus is only on authorizations/permissions and limits set out in legislation and regulations—the statutory “rules” for handling data—that apply to SDU activities and SDU “bodies” to which the statute applies. This level of analysis was necessary, given the goal of the scan.</td>
</tr>
<tr>
<td>Some of the Elements in the CIHR Best Practices compendium are not clearly applicable to SDU activities. For these Elements (Element 3—Determining if consent is required; Element 4—Managing and documenting consent; Element 5—Informing prospective research participants about the research; Element 6—Recruiting prospective research participants), only a brief rationale—a memory prompt—was included for why the Element is not applicable to SDU.</td>
</tr>
<tr>
<td>Some of the Element titles have been modified to provide a better fit with the characteristics of SDU.</td>
</tr>
<tr>
<td>As much as possible, the rules for collection, use and disclosure have been separated, as some SDU entities collect and use information for SDU, but do not disclose information; or, collect and disclose information for SDU, but do not use information for SDU (i.e. not all SDU entities “do” research.)</td>
</tr>
</tbody>
</table>

Summary

**Key Message - Most important...**

Participants unanimously supported the idea that a Privacy Best Practices for SDU will not work unless it brings clarity to the law as it applies to secondary data research without consent. Preferentially, researchers would like the “checklist” approach to privacy: √ do this or; × don’t do that.
The Privacy Best Practices for SDU is in plain — not legal — language. On the left-hand side of the page is a distillation of what the law requires (from the Encyclopedia and Translation Document) across Canada’s provinces and territories to protect the privacy of individuals whose health information is used for SDU research (statistical/epidemiological/population-based/HSPR). The right-hand column contains policies, practices and procedures gathered from institutes and centres across Canada that will enable organizations and researchers using secondary data to craft the appropriate policies and practices for their jurisdiction and research culture (from the Privacy Toolkit and Templates). Many of these templates have the added feature of already having been vetted by their local privacy oversight bodies.

The objectives of the Phase III Workshop were two-fold:

1. To discuss and finalize a Privacy Best Practices for SDU for those institutes and agencies whose research methods include the use of data collected for another purpose (secondary use of data) without consent that will serve multiple purposes:
   a. Research environments and researchers who employ the Best Practices will “prove” that a high standard of data security and privacy protection is in place in their workplace.
   b. Use of the Best Practices also certifies that there is due diligence at a research “site” – that there is concordance with local legislation and good internal-to-site standards (policies, procedures, security).
   c. Adherence of research organizations to the Best Practices could facilitate and produce broader support for this type of research by being acceptable to provincial Privacy Commissioners/Ombudsman, data stewards, and Research Ethics Boards (REBs).
   d. Additionally, the Best Practices may enable REBs and Privacy Commissioners/Ombudsman to reduce time and resources spent on estimating how “safe” and “low-risk” these institutes/agencies are when reviewing proposals for research in the public good.
   e. Institutes complying with the Best Practices could additionally lend themselves more easily to the possibility of creating and or making available more public use data (contingent on funding and approvals) as recommended in the final data report.

2. To further develop and operationalize the Privacy Best Practices for SDU a number of collaborators and SDU agencies offered to pilot the Best Practices. A Privacy Checklist was also developed to facilitate the piloting process. One agency has already successfully employed the strategy for creating their own best practices. The comments received from the pilot sites were incorporated in to the final documents and Tools (see Appendix 10).

The workshop provided a collegial forum for discussion of the draft voluntary privacy standard and the companion documents. The speakers provided background information which informed the discussions. Reasonable consensus was reached on the contents of the ten elements and suggestions were made for some additional information for the toolkit.

Population-based health and health services databases and their potential for use in innovative, vital health research in Canada requires the Tools that were developed through these workshops. These Tools will facilitate and create opportunities for national
Harmonizing Research & Privacy: Standards for a Collaborative Future.
Privacy Best Practices for Secondary Data Use (SDU)

collaboration. They are Tools which are essential to assist in the planning of strategic investments in population health and secondary data use research.

Recommendations

The Privacy Best Practices for SDU and Toolkit represents a major initial investment by the collaborating group and CIHR-IHSPR (and other CIHR Institutes). To maximize the return on this investment we make the following recommendations:

1. In order to ensure that the Workshop Tools - Privacy Best Practices for SDU, Toolkit, Checklist and Reference materials remain useful, there needs to be a commitment to a mechanism for updating, modifying and supporting this collective work. These Tools are living, not static, documents. As technology evolves, statutory obligations are modified and practices and standards change – the Privacy Best Practices for SDU and Toolkit will require updating.

2. Workshop participants were interested in developing an arbitration mechanism for use when privacy and research activity (specifically with REBs) are at odds. Additionally, there is interest in regional or provincial SDU-specific REBs with standing which could provide expertise for review of these types of projects, as there are some researchers who lack access to appropriate non-consent based expertise.

Both these valuable suggestions were outside the scope of this particular project, but would seem an appropriate issue for CIHR Ethics group to consider.

While more than one statute in a given province or territory may dictate required levels of protection for personal information, we selected statutes to include in the Encyclopedia that set the highest bar and/or provided most detail for establishing privacy protections within policy among the main participating organizations for the workshops. Other statutes that have been reviewed in a similar fashion (but are not included in the Encyclopedia) to ensure consistency with the Privacy Best Practices for SDU are FIPPA (Ontario), PIPA (BC), FOIPPA (Alberta), FIPPA (Saskatchewan) and PIPEDA (Canada.)

The third workshop generated significant interest in having the other statutes mentioned above analyzed and included in the Encyclopedia. Some have suggested the analysis should also reflect findings of Privacy Commissioners and other similar statutory oversight authorities; as such findings are important references for interpreting statutory requirements.

Additionally, some organizations governed only by one of the other statutes mentioned (and not by health information specific legislation) told us that they have gone beyond their

12 For example, the Manitoba Centre for Health Policy is governed by both the Personal Health Information Act (PHIA) and the Freedom of Information and Protection of Privacy Act (FIPPA.) However, PHIA sets a higher standard for research and is the basis for MCHP policy. Therefore, PHIA was included in the scan and FIPPA was reviewed to ensure there are not inconsistencies between the guidance in the Privacy Best Practices for SDU and requirements for FIPPA.
statutory obligations and implemented higher protections as a matter of policy that, once adopted, is binding upon them. They recommended incorporating an analysis of this type of material in parallel to the Encyclopedia.

3. As a result of the overwhelming response regarding the utility of the Encyclopedia, we recommend that support be provided for continued analysis of relevant statutory materials, as well as binding policies and interpretations of statutory requirements within the findings/orders of statutory oversight authorities.

Key Message – Recommendations

The Privacy Best Practices for SDU and Toolkit represents a major initial investment by the collaborating group and CIHR-IHSPR (and other CIHR Institutes). To maximize the return on this investment we make the following recommendations:

1. To ensure that the Workshop Tools - Privacy Best Practices for SDU, the Toolkit, Checklist and the Reference Materials remain current and useful, there needs to be a commitment to a mechanism for updating, modifying and supporting this collective work. These Tools are living, not static, documents. As technology evolves, statutory obligations are modified and practices and standards change – the Privacy Best Practices for SDU and Toolkit will require updating.

2. Workshop participants were interested in developing an arbitration mechanism for use when privacy and research activity (specifically with REBs) are at odds. Additionally, there is interest in regional or provincial SDU-specific REBs with standing which could provide expertise for review of these types of projects, as there are some researchers who lack access to appropriate non-consent based expertise.

3. As a result of the overwhelming response regarding the utility of the Encyclopedia, we recommend that support be provided for continued analysis of relevant statutory materials, as well as binding policies and interpretations of statutory requirements within the findings/orders of statutory oversight authorities.

We are grateful to CIHR-IHSPR and sister agencies for their support of this project. We also thank our SDU research colleagues across Canada and privacy oversight authorities who provided support and guidance for this undertaking.
Appendix 1: List of Funding Agencies

Funding Partners for this Initiative (Workshops I, II and III) include:

Canadian Institute for Health Research (CIHR) Institutes:

Institute of Health Services and Policy Research
Institute of Aboriginal Peoples Health
Institute of Genetics
Institute of Population and Public Health
Institute of Neurosciences, Mental Health and Addiction
Institute of Human Development, Child and Youth Health
Institute of Aging
Institute of Nutrition, Metabolism and Diabetes
Institute of Cancer Research
CIHR Ethics Office

As well as:
Canadian Institute for Health Information (CIHI) Canadian Population Health Initiative
Canadian Health Services Research Foundation
Canadian Patient Safety Institute

Additional funding provided by:
Weir Foulds LLP Health Law Group, Toronto ON
Aikins, MacAulay, Thorvaldson LLP, Winnipeg, MB
APPENDIX 2  List of all (Phase I, II & III) Workshop Participants:

Agnew, Alex  
Director of Corporate Services  
Health Quality Council  
241 - 111 Research Drive,  
Saskatoon, SK, S7N 3R2  
(306) 668-8810 ext. 120  
Aagnew@HQ.sk.ca

Barre, Louis  
Director, Health Information Management  
Manitoba Health  
300 Carlton Street  
Winnipeg, MB R3B 3M9  
(204) 786-7139  
(204) 944-1911  
lbarre@gov.mb.ca

Bartlett-Esquiland, Dr. Gillian  
McGill University  
Royal Victoria Hospital  
Dept. of Medicine,  
Clinical Health and Informatics Research  
Morrice House  
1140 Pine Ave.  
Montreal, QC H3A 1A1  
(514) 934-1934 Ext. 32979  
gillian.bartlett@mcgill.ca

Black, Charlyn  
Director  
Centre for Health Services & Policy Research  
429 - 2194 Health Sciences Mall  
Vancouver, BC V6T 1Z3  
(604) 822-6030  
(604) 822-1370  
cblack@chspr.ubc.ca

Brown, Ken  
Health Research Ethics Board,  
Faculty of Medicine,  
University of Manitoba  
P126-770 Bannatyne Campus  
Winnipeg, Manitoba R3E 0W3  
brownk@cc.umanitoba.ca

Bower, Peter  
Executive Director  
Access & Privacy  
Office of the Ombudsman  
750 - 500 Portage Avenue  
Winnipeg, MB R2H 0M2  
(204) 982-9130  
(204) 942-7803  
pbower@ombudsman.mb.ca

Burchill, Charles  
Senior Systems Analyst  
Manitoba Centre for Health Policy  
Dept of Community Health Sciences,  
University of Manitoba  
408 - 727 McDermot Avenue  
Winnipeg, MB R3E 3P5  
(204) 789-3429  
(204) 789-3910  
charles_burchill@umanitoba.ca

Carr, RJ  
Policy Analyst  
Government of Nunavut  
Department of Health & Social Services  
PO Box 1000, Station 1000  
Iqaluit NU X0A 0H0  
(604) 822-5059  
(604) 822-5690  
Rcarr@gov.nu.ca

Carrick, David  
Aikins, MacAulay & Thorvaldson LLP  
30th Floor Commodity Exchange Tower  
360 Main Street  
Winnipeg, MB R3C 4G1  
dmc@aikins.com

Carson, Tom  
Member of the Public  
90 Meadow Ridge Drive  
Winnipeg, MB  
(204) 269-4553  
tcarson@mts.net
Harmonizing Research & Privacy: Standards for a Collaborative Future.
Privacy Best Practices for Secondary Data Use (SDU)

Cavoukian, Ann
Privacy Commissioner of Ontario
Office of the Information and Privacy Commissioner of Ontario
80 Bloor St West, Suite 1700
(867) 975-5718
(867) 975-5733
commissioner@ipc.on.ca

Chapman, Sheila
Project Manager - Privacy Initiative
CIHR Institute of Health Services & Policy Research
410 Laurier Ave. West 9th Floor,
209A Ottawa, ON K1A 0W9
(613) 954-1803
(613) 941-1040
schapman@cihr-irsc.gc.ca

Collins, Paulette
Senior Administrator
Manitoba Centre for Health Policy
Dept of Community Health Sciences,
University of Manitoba
408 - 727 McDermot Avenue
Winnipeg, MB R3E 3P5
(204) 975-7730
(204) 789-3910
paulette_collins@cpe.umanitoba.ca

Choptain, Katherine
Chief Privacy Officer
Winnipeg Regional Health Authority
1800 – 155 Carlton Street
Winnipeg, MB R3C 4Y1
(204) 926-7049
(204) 926-7007
KChoptain@wrha.mb.ca

Cronin, Gerarda
Director of Quality and Decision Support,
Child Health Program,
Winnipeg Regional Health Authority
Associate Professor and Associate Head,
Department of Pediatrics and Child Health,
University of Manitoba AE102
671 William Avenue
Winnipeg, MM R3A 1R9

Dickson, R. Gary,
Saskatchewan Information and Privacy Commissioner
100-1230 Blackfoot Drive
Regina, Sask S4S 7G4
(306) 798-1601
(306) 798-1603
gdickson@oipc.sk.ca

Dowler, Judith
Health Canada
Health Care & Issues Div.
Health Promotion and Programs
Ottawa, ON K1A 1B4
(613) 941-7561
(613) 948-2110
judith_m_dowler@hc-sc.gc.ca

El Emam, Khaled
Associate Professor
CRC in Electronic Health Information
CHEO Research Institute
401 Smyth Road,
Ottawa, ON K1H 8L1
(613) 738-4181
(613) 745-2913
kelemam@uottawa.ca

Gagnon, Diane
Senior Program Officer
Granting and Commissioning
Canadian Health Services Research Foundation
700 – 1565 Carling Avenue
Ottawa, ON K1Z 8R1
(613) 728-2238
(613) 728-3527
diane.gagnon@chsrf.ca

Gibson, Elaine
Associate Professor/Associate Director
Health Law Institute
Dalhousie Law Faculty 6061 University Avenue
Halifax, Nova Scotia B3H 4H9
(902) 494-6882
(904) 494-6879
Elaine.gibson@dal.ca

Gideon, Valerie
Director, First Nations Centre
National Aboriginal Health Organization
130 Albert Street, Suite 1500
Ottawa, ON K1P 5G4
(613) 233-1543 Ext. 501
Direct (613) 566-5970
(613) 233-1853
vgideon@naho.ca
Harmonizing Research & Privacy: Standards for a Collaborative Future.
Privacy Best Practices for Secondary Data Use (SDU)

Grant, Debra
Research Officer
Privacy Commissioner of Ontario
80 Bloor Street West, Suite 1700
Toronto, ON  M5S 2V1
(416) 326-3333
(416) 325-9195
dgrant@ipc.on.ca

Grund, Darrin
Data Warehouse Manager
Faculty of Health Sciences
Simon Fraser University
8888 University Drive
Burnaby, BC V5A
dmgrund@sfu.ca

Guinchard, Ann
Privacy Officer and
Director of Information Policy and Analysis
Policy and Planning Branch
Saskatchewan Health
3475 Albert Street
Regina, SK  S4S 6X6
(306) 787-3160
(306) 787-2974
aguinchard@health.gov.sk.ca

Herbert, Carole
Manager, ON Cancer Registry & Privacy Officer
Cancer Care Ontario
620 University Ave.
Toronto, ON  M5G 2L7
(416) 217-1245
(416) 971-6888
Carole.Herbert@cancercare.on.ca

Hamilton, Irene
Ombudsman Manitoba
Office of the Ombudsman
750 - 500 Portage Avenue
Winnipeg, MB R3C 3X1
(204) 982-9130
(204) 942-7803
ihamilton@ombudsman.mb.ca

Hayes, Michael
Associate Dean
Faculty of Health Sciences
Simon Fraser University
8888 University Drive
Burnaby, BC V5A 1S6
(604) 268-6648
(604) 291-5927
mhayes@sfu.ca

Hirtle, Marie
Privacy Consultant
Biokit Inc. Recherche & Conseil Research & Consulting
50, Avenue Dobie
Mont-Royal, Québéc H3P 1R8
514-734-0225
hirtlem@sympatico.ca

Hogg-Johnson, Sheilah
Senior Scientist and Manager
Institute for Work & Health
481 University Ave., Suite 800
Toronto, ON M5G 2E9
(416) 927-2027 ex. 2130
(416) 927-4167
shoggjohnson@iwh.on.ca

Howard, Rosalyn
Director
Learning and Development Services
University of Manitoba
511 Drake Centre
Winnipeg, MB
(204) 474-7389
rosalyn_howard@umanitoba.ca

Hutchison, Brian
Director, CHEPA
McMaster University
1200 Main Street West
Hamilton, ON L8N 3Z5
(905) 525-9140 Ext. 22123
(905) 545-5211
hutchb@mcmaster.ca

Jackson, Phil
Director Health Information Privacy Branch
Ministry of Health and Long-Term Care
101 Bloor Street West
Toronto, ON  M5S 2Z7
(416) 327-4395
(416) 314-8275
phil.jackson@moh.gov.on.ca

Kendall, Ora
Chief, Data Development & Exchange Program
Population & Public Health Branch, Health Canada
130 Colonnade Rd., Rm 371A,
Nepean ON K1A 0K9
(613) 954-2268
(613) 957-6218
Ora_Kendall@hc-sc.gc.ca
Harmonizing Research & Privacy: Standards for a Collaborative Future. 
Privacy Best Practices for Secondary Data Use (SDU)

Kephart, George  
Director, Population Health Research Unit 
Dalhousie University 
Community Health and Epidemiology 
5849 University Avenue 
Halifax, NS  B3H 4H7 
(902) 494-5193  
(902) 494-1597  
George.Kephart@dal.ca

Kosseim, Patricia  
Acting Director, Ethics Office 
Canadian Institutes for Health Research 
410 Laurier Ave. West 9th Floor, 
209A Ottawa, ON  K1A 0W9 
(613) 954-1801  
(613) 941-1040  
P.Kosseim@cihr.ca

Larsen, Craig  
Institute Manager 
CIHR Institute of Health Services & Policy Research 
209 - 2150 Western Parkway 
Vancouver, BC V6T 1V6 
(604) 222-6874  
(604) 224-8635  
clarsen@ihspr.ubc.ca

Laupacis, Dr. Andreas  
President & CEO 
Institute for Clinical Evaluative Sciences 
G106 - 2075 Bayview Avenue 
Toronto, ON  M4N 3M5 
(416) 480-4297  
(416) 480-6048  
alaupacis@ices.on.ca

Le Petit, Christel  
Chief, Occupational and Environmental Health, 
Research Section 
Health Statistics Division 
Main 2200, Statistics Canada 
Tunney's Pasture 
Ottawa, On K1A 0T6 
613-951-3856  
613-951-0792  
Christel.LePetit@statcan.ca

Lix, Lisa  
Researcher 
Manitoba Centre for Health Policy 
Dept of Community Health Sciences, 
University of Manitoba 
408 - 727 McDermot Avenue 
Winnipeg, MB  R3E 3P5 
(204) 975-7799  
(204) 789-3910  
lisa_lix@cpe.umanitoba.ca

McDonald, Lucy  
Director of Communications & Privacy 
Newfoundland & Labrador Centre for Health Information 
1st Floor Crosbie Bldg., 
1 Crosbie Place 
St. John's, NL  A1B 3Y8 
(709) 757-2424  
(709) 757-2411  
lucym@nlchi.nf.ca

McGrail, Kimberlyn  
Research Associate 
Centre for Health Services and Policy Research 
429 - 2194 Health Sciences Mall 
Vancouver, BC  V6T 1Z3 
(604) 822-8044  
(604) 822-1370  
kmgrail@chspr.ubc.ca

Meagher, Nancy  
Executive Director 
Population Health and Learning Observatory 
320 - 2206 East Mall, 
Library Processing Centre, 
Vancouver, BC  V6T 1Z3 
(604) 822-1370  
(604) 822-0640  
nancy@phlo.ubc.ca

Martens, Patricia  
Director 
Manitoba Centre for Health Policy 
Dept of Community Health Sciences, University of Manitoba 
408 - 727 McDermot Avenue 
Winnipeg, MB  R3E 3P5 
(204) 789-3791  
(204) 789-3910  
pat_martens@cpe.umanitoba.ca
Harmonizing Research & Privacy: Standards for a Collaborative Future.
Privacy Best Practices for Secondary Data Use (SDU)

McLaren, Heather
Director, Legislative Unit
Manitoba Health
1046 - 300 Carlton Street
Winnipeg, Manitoba ReB 2K6
(204) 788-6613
hmclaren@gov.mb.ca

Mustard, Cam
President and Scientific Director
Institute for Work & Health
481 University Ave.,
Suite 800
Toronto, ON  M5G 2E9
(416) 927-2027 Ext. 2143
(416) 927-4167
cmustard@iwh.on.ca

Neill, Andrea
Chief Privacy Officer
Canadian Institute for Health Information
377 Dalhousie Street
Ottawa, ON K1N 9N8
(613) 241-7860
(613) 241-8120
aneill@cihi.ca

Noseworthy, Dr. Tom
Professor and Head,
Dept of Community Health Sciences
Director, Centre for Health and Policy Studies
University of Calgary
3330 Hospital Drive NW
Calgary, AB T2N 4N1
(403) 220-2481
(403) 270-7307
tnosewor@ucalgary.ca

Perry, Gail
Access & Privacy,
Office of the Ombudsman
750 – 500 Portage Avenue
Winnipeg, MB R3C 3X1
(204) 982-9130
(204) 942-7803
gperry@ombudsman.mb.ca

Pullman, Daryl
Associate Professor of Medical Ethics
Memorial University of Newfoundland
Faculty of Medicine
300 Prince Philip Drive
St. John’s, NL A1B 3V6
(709) 777-6220
(709) 777-7382
dpullman@mun.ca

Rempl-Rossum, Shelley
Health Research Ethics Board,
Faculty of Medicine,
University of Manitoba
P126-770 Bannatyne Campus
Winnipeg, Manitoba R3E 0W3
(204) 789-3389
remross@ms.umanitoba.ca

Ries, Nola
Research Associate/Project Manager
Health Law Institute, Law Centre,
University of Alberta
Edmonton, AB T6G 2H5
(780) 492-7577
(780) 492-9575
nries@law.ualberta.ca

Robens Paradise, Yoel
Director, Health Record Services
St. Paul's Hospital
1081 Burrard Street
Vancouver, BC V6Z 1Y6
(604) 806-9098
(604) 806-9006
yparadise@providencehealth.bc.ca

Roch, Joan
Chief Privacy Strategist
Canada Health Infoway
1000, rue Sherbrooke Ouest, Suite 1200
Montreal, QC H3A 3G4
Toll free: 1-866-868-0550
Fax: (514) 868-1120
jroch@infoway-inforoute.ca

Roos, Noralou
Professor and Director
Manitoba Centre for Health Policy
Dept of Community Health Sciences,
University of Manitoba
408 - 727 McDermot Avenue
Winnipeg, MB R3E 3P5
(204) 789-3319
(204) 789-3910
noralou_roos@cpe.umanitoba.ca

Samis, Stephen
Manager, Research, Analysis and Infrastructure
CPHI Secretariat
377 Dalhousie St., Ste. 200
Ottawa, ON K1N 9N8
613-241-7860 Ext. 4129
613-241-8120
ssamis@cihi.ca
Harmonizing Research & Privacy: Standards for a Collaborative Future.
Privacy Best Practices for Secondary Data Use (SDU)

Schnarch, Brian
National Aboriginal Health Organization
220 Laurier Avenue West, Suite 1200,
Ottawa, ON K1P 5Z9
(613) 566-5973
(613) 237-1810
bschnarch@naho.ca

Slaughter, Pam
Senior Research Coordinator and Privacy Officer
Institute for Clinical Evaluative Sciences (ICES)
G Wing, 2075 Bayview Avenue
Toronto, ON M4N 3N5
(416) 480-4055 Ext. 1-3886
(416) 480-6048
pam@ices.on.ca

Shortt, Dr. Samuel
Director
Centre for Health Services and Policy Research
Queen's University
Kingston, ON K7L 3N6
(613) 533-6387
(613) 533-6353
seds@post.queensu.ca

Smith, Mark
Director, Population Health Research Unit
Dalhousie University Community Health and Epidemiology
5849 University Avenue
Halifax, NS B3H 4H7
(902) 494-6456
(902) 494-1597
Mark_Smith@dal.ca

Spencer, Pamela
Provincial Vice-President,
Corporate Affairs and General Counsel
Cancer Care Ontario
620 University Ave.
Toronto, ON M5G 2L7
(416) 217-1233
cel: (416) 670-3136
(416) 217-1249
pamela.spencer@cancercare.on.ca

Stranc, Leonie
Decision Support Services
Manitoba Health
300 Carlton St.
Winnipeg, MB R3M 3M9
(204) 786-7204
(204) 772-7213
lstranc@gov.mb.ca

Sullivan, Dr. Terry
Vice President, Research & Cancer Control
Cancer Care Ontario
620 University Ave.
Toronto, ON M5G 2L7
(416) 217-1244
(416) 217-1243
terry.sullivan@cancercare.on.ca

Tamblyn, Dr. Robyn
Epidemiologist
McGill University
Royal Victoria Hospital
Div. Of Epidemiology and Biostatistics
Room 4.11
Montreal, Quebec H3A 1A1
(514) 842-1231 Ext. 6902
(514) 843-1493
robyn.tamblyn@mcgill.ca

Tarshis, Debbie S.
Partner
Weir Foulds LLP
The Exchange Tower, Suite 1600
PO Box 480, 130 King St. W.
Toronto, ON M5X 1J5
(416) 947-5037
(416) 365-1876
dtarshis@weirfoulds.com

Thornhill, Jennifer
Student Intern
Ethics Review of Applied health Services
Canadian Health Services Research Fundation
700 – 1565 Carling Avenue
Ottawa, ON K1A 8R1
(613) 728-2238
(613) 728-3527
jennifer.thornhill@chsrf.ca

Tkachenko, Laurisa
Director, Privacy Office
Workplace Safety & Insurance Board
200 Front Street West, 20th floor
Toronto, ON
(416) 344-3685
laurisa_tkachenko@wsib.on.ca

Tu, Jack
Senior Scientist
Institute for Clinical Evaluative Sciences
G106 - 2075 Bayview Avenue
Toronto, ON M4N 3M5
(416) 480-6083
(416) 480-6048
tu@ices.on.ca
Appendix 3: List of Steering Committee Members

Dr. Ken Brown (Manitoba)
Dr. Kim McGrail (BC)
Dr. Mark Smith (NS)
Dr. Noralou Roos (Manitoba)
Dr. Robyn Tamblyn (Quebec)
Dr. Debra Grant (Ontario)
Dr. Linda Van Til (PEI)
Paulette Collins (MCHP)
Pam Slaughter (ICES)
Roslyn Howard (facilitator) - listener

This committee met twice via teleconference – once in October 2006 and once in November 2006.
Appendix 4: Steering Committee teleconferences

The main outcomes of the October meeting included:

- Agreement that the structure of the developing framework for the Privacy Best Practices will follow the CIHR Best Practices for Protecting Privacy in Health Research, September 2005 document element-by-element to facilitate usability between the documents.
- The legal analysts had found tremendous differences in interpretation/definitions, validating the plan from Workshops I & II to create a Table of Equivalencies.
- Agreed that the plan to conduct an email survey of a sample of research organizations throughout Canada who conduct SDU will validate the legislative acts that are routinely used – this will ensure a workshop outcome is meeting requirements.
- The Steering Committee provided the following updates to the May 2004 voluntary privacy standard for SDU:
  - Add an initial threat risk assessment (TRA) / penetration assessment (in some form) - as a basis line and then periodically. TRA could be comforting for custodians as well as research colleagues. Should not be the size of the organization but the sensitivity of the data held that puts this into play.
  - Need a separate piece on data security and safeguards: physical data protection / intrusion detection / electronic safeguards.
  - Add clarity to the privacy impact assessment: one project-specific and one organizational-/system-specific – project-specific privacy review and PIA = systems or database privacy assessment.
  - Add clarity to the Research agreement. Develop standard templates for data and researcher agreements.
  - Add clarity to the transparency requirement and define the roles of custodian, user / researcher and provider / stewards.
  - Define the difference between ‘access’ and ‘disclosure’.
  - Plain, useable language was an imperative. While it was acknowledged that this will be challenging as the document is based on legal language, efforts will be made to keep the language simple, the documents user-friendly and restrict the legal language to the Statute-by-Statute Analysis document.
  - The focus of the document is to be a useful, workable document that facilitates the transfer of knowledge in the most effective way.
  - The objective of the legal scan has been establishing what the minimal standards might be; legislative change is not being sought – this is intended as a policy document.
  - The importance of establishing these standards was reaffirmed. There needs to be a baseline/foundation that everyone starts with, some minimal best practices that everyone who works with secondary data without consent utilizes.
  - To create best practices, everyone must start from the same terms of reference. In order to start at this point, the Table of Definitions and Equivalent Terms has been developed.
Discussion about the abundant opportunity for knowledge transfer, how to communicate information to data stewards and data centers and, perhaps most importantly, how to educate the public and the community.

Interest expressed in developing a SDU specific Research Ethics Board (REB). It was felt that this would ensure that the REB was familiar with the rules and regulations of SDU without consent and inform data owners.

The November meeting was spent discussing the draft documents which had been provided to the committee for review.

The documents consisted of:

1. Background to HSPR-specific legislative scan—summary of activities to date
2. Sample of Phase 1 analysis
   - Manitoba—Personal Health Information Act (PHIA)
3. Table of Contents for the HSPR-specific legislative scan
4. Sample excerpts from the scan
   - Table B.4—Definitions/equivalent terms—Identifiability
   - Sample excerpt from the “Voluntary Standard Workbook” (Table for Element 8.1—Use)

Discussions were focused on the format of the materials; the structure of the analysis; and the proposed structure for the January 2006 workshop material.

The discussion identified that there were two sections found to be slightly confusing: the first was where elements were identified but tables explaining this element weren’t found until much later on in the document; second, the HMS terminology. It was determined that these will be clarified in the preamble to the documents and each section for the workshop documents.

Overall there were sentiments of amazement at the amount of time and effort that was put into this research, with certainty that it will be incredibly useful.

The core working group pointed out that:

- the format of the documents may change slightly as they are evolving documents,
- the legislation doesn’t provide clear direction in all provinces.

The legal consultants will obtain feedback from each jurisdiction before the final report is submitted.

It was pointed out how much information these documents entail and that it will be a challenge to cover it all at the workshop and maintain discussions. As such the workshop agenda will be restructure to better facilitate the required flow of discussions. It was also suggested that perhaps a topic at the workshop should include discussion about the abundant opportunity for knowledge transfer, how to communicate information to data stewards, data centres, the public and the community.
Appendix 5: Email Survey

To identify “Key statutes” the following Organizations were asked via an email survey the following:

“Assuming privacy legislation is the foundation from which all jurisdictions work, in your institute’s research operations what are the legislative Acts that you routinely use to ensure your work is meeting legislative requirements?”

The results are presented in the table below.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Jurisdiction</th>
<th>Replied</th>
<th>Key Statute(s)</th>
<th>Other Statute(s) [don’t raise the bar]</th>
<th>Statutes Included*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centre for Health Services &amp; Policy Research</td>
<td>BC</td>
<td>YES</td>
<td>FOIPPA</td>
<td>PIPA, PIPEDA</td>
<td>FOIPPA</td>
</tr>
<tr>
<td>Centre for Health and Policy Studies, University of Calgary</td>
<td>AB</td>
<td>NO</td>
<td></td>
<td></td>
<td>HIA</td>
</tr>
<tr>
<td>Health Quality Council</td>
<td>SK</td>
<td>YES</td>
<td>HIPA</td>
<td>FIPPA, PIPEDA</td>
<td>HIPA</td>
</tr>
<tr>
<td>Manitoba Centre for Health Policy, University of Manitoba</td>
<td>MB</td>
<td>YES</td>
<td>PHIA</td>
<td>FIPPA, PIPEDA</td>
<td>PHIPA</td>
</tr>
<tr>
<td>Institute for Work &amp; Health; Institute for Clinical Evaluative Sciences (ICES); and CHEPA McMaster University</td>
<td>ON</td>
<td>YES</td>
<td>PHIPA, FIPPA</td>
<td>FIPPA, PIPEDA</td>
<td>PHIPA</td>
</tr>
<tr>
<td>Clinical Health Information Research Centre</td>
<td>QC</td>
<td>YES</td>
<td>Loi sur l’accès</td>
<td>LSSS LAM</td>
<td>Loi sur l’accès LSSS LAM</td>
</tr>
<tr>
<td>Population Health Research Unit, Dalhousie, Univ</td>
<td>NS</td>
<td>YES</td>
<td>FoIPPA</td>
<td></td>
<td>FoIPPA</td>
</tr>
<tr>
<td>NFLD &amp; Labrador Centre for Health Information; Health Policy &amp; Health Care Delivery Faculty of Medicine</td>
<td>NL</td>
<td>YES</td>
<td>PIPEDA, CDSA, FDA</td>
<td>HA, ATIPPA CHIA, CDSA, FDA, CTRFA, CDA, ECA, RIHAA, HIA</td>
<td>ATIPPA, HA, CHIA</td>
</tr>
<tr>
<td>PEI Department of Health and Social Services</td>
<td>PEI</td>
<td>NO</td>
<td></td>
<td></td>
<td>FIPPA</td>
</tr>
</tbody>
</table>

FOIPPA – Freedom of Information and Protection Act, 1996 – British Columbia (BC)
HIA – Health Information Act, 1996 – Alberta (AB)
HIPA – The Health Information Protection Act, 2003 – Saskatchewan (SK)
PHIA – Personal Health Information Act, 1997 – Manitoba (MB)
PHIPA – Personal Health Information Protection Act, 2004 – Ontario (ON)
Loi sur l’accès – Personal Information – Québec (QC)
LSSS – Health and Social Services – Québec (QC)
LAM – Health Insurance Act – Québec (QC)
FoIPPA – Freedom of Information and Protection of Privacy Act, 1999 – Nova Scotia (NS)
ATIPPA – Access to Information and Protectin of Privacy Act, Newfoundland & Labrador (NL)
HA – Hospital Act, Newfoundland & Labrador (NL)
CHIA – Centre for Health Information Act, Newfoundland & Labrador (NL)
Appendix 6 – Phase III Workshop Agenda.

“Harmonizing Research & Privacy: Standards for a Collaborative Future. Creating Consensus for a Privacy Voluntary Standard for HSPR (Phase III)”

Inn at the Forks Hotel, Winnipeg, Manitoba
January 16 & 17, 2006

Day 1: Setting the Stage

0830 Registration/Continental Breakfast

0900 Pat Martens: Director, Manitoba Centre for Health Policy: Welcome

0905 Pam Slaughter and Paulette Collins: “Why We’re Here and What We Want to Accomplish in Phase III”.

0920 Irene Hamilton, Ombudsman, Manitoba
Gary Dickson, Information and Privacy Commissioner, Saskatchewan
Debra Grant, Sr. Health Policy Analyst, Office of the Information and Privacy Commissioner of Ontario

“Perspectives on voluntary good practice standards from the oversight bodies”.


1020 Don Willison: “Privacy and health research: What are the attitudes of the public?”

1040 Clarifying questions

1045 Coffee Break (15 minutes)

1100 Facilitated Discussion
Karen Weisbaum and Marie Hirtle. “The Rules in a Box: Overview of the legislative landscape specific to HSPR”

1215 Lunch (45 minutes)

1300 Facilitated Discussion

“Choosing good practices: implications for creating a voluntary standard”. Elements 1-4 (Elements 5 & 6 not directly applicable to HSPR)

1500 Refreshment Break (15 minutes)

1515 Facilitated Discussion

“Choosing good practices: implications for creating a voluntary standard”.
Elements 7-10

1700 Adjournment Day 1
Day II Discussions: Finalizing the Draft Standard

0800 Continental Breakfast

0830 Welcome Day 2 and Housekeeping Issues
0845 – 1030 Sober second thoughts: Choosing Good Practices
Facilitated Discussion

1030-1100 Coffee Break

1100 – 1230 Paulette Collins & Pam Slaughter: “What’s in the Toolkit? Administrative, technological and physical elements”

1230 – 1330 Lunch

1330 - 1500 Facilitated Discussion: Consolidating the “Good Practices” and the HSPR Privacy Toolkit

1500 - 1600 Piloting the draft Voluntary Standard in Canadian HSPR
Facilitated Discussion

1600 Next steps

1630 Adjournment
Appendix 7: Decision Tree

1. Is it health research?
   - **YES**: Proceed to the next question
   - **NO**: Is it research involving secondary use of data? (Data collected for other purposes)?

2. Is it research involving secondary use of data? (Data collected for other purposes)?
   - **YES**: Proceed to the next question
   - **NO**: Does the research involve large population samples or cohorts?

3. Does the research involve large population samples or cohorts?
   - **YES**: Proceed to the next question
   - **NO**: Is consent impracticable?

4. Is consent impracticable?
   - **YES**: This research can follow the SDU standard
   - **NO**: Refer to the CIHR Privacy Best Practices*

---

*Canadian Institutes of Health Research (CIHR). Best Practices for Protecting Privacy in Health Research. September 2005*
Appendix 8: Summary of Workshop Tools

**Privacy Best Practices for Secondary Data Use (SDU)**
This document provides the foundation for ensuring respectful use of secondary data. It lays out, in plain language on the left-hand side of the page, a distillation of legislative requirements across Canada’s provinces and territories to protect the privacy of individuals whose health information is used for SDU research. The right-hand column contains titles of templates for policies, practices and procedures contained in the Privacy Toolkit. This document is founded on the Reference materials below – the Translation document Rules in a Box which originates from the Encyclopedia - Statutes-by-Statutes Analysis.

**Privacy Toolkit for SDU (secured and non-secured environments)**
The Toolkit and companion Templates provide users with a range of appropriate options - methods for actions that will meet the legislative requirements. These documents are offered as templates, by active researchers, for your use. You are invited to borrow liberally from these, or use them as a platform to develop your own policies, practices and procedures. Organizations and researchers are encouraged to create and tailor a practical application of the Privacy Best Practices for SDU that is appropriate to their local research culture and legislative requirements. You are asked to acknowledge the originating organization in any document created from or if using a template.

**Checklist for Privacy Best Practices for SDU**
The Checklist provides another tool for SDU organizations/researchers to use to create and record an inventory of SDU privacy best practices, by prompting the formalization in written form of all necessary policies and procedures. For those who want to apply the Best Practices for SDU, it's a method to record/monitor/facilitate the application and use of the Best Practices and can help construct the ‘big picture’ for your organization or project.

**REFERENCE MATERIALS (Appendices)**

**Encyclopedia - Statute-by-Statute Analysis of Privacy Legislation Relevant to Secondary Data Use Organizations by Jurisdiction** - an analysis
This document contains an analysis of the relevant provisions of each key statute by province/territory and provides a readable interpretation of legislation and regulations specific to SDU. Each analysis follows the same categories (Elements) as the CIHR Best Practices for Protecting Privacy in Health Research, allowing for comparison with the CIHR document.

PI (Personal Information) and PHI (Personal Health Information) are acronyms used throughout the analysis. Not all statutes use the same terms or discriminate between personal information and personal health information. The language used reflects that found in the statutes.

**The Translation - The Rules in a Box**
This document contains the same material as in the statute-by-statute analysis, but it is organized according to the categories/elements in the CIHR Best Practices for Protecting Privacy in Health Research document. Analysis of the relevant statutory provisions for each province/territory are in the left-hand column, while the right-hand column provides non-legal language points – translating and distilling the analysis into concise policy requirements. These policy requirements form the basis of Privacy Best Practices for SDU.

**The Dictionary - Table of Definitions and Equivalent Terms**
This document contains the ten frequently-used concepts that have been identified and the corresponding terms/definitions from each jurisdiction. This provides readers with a basis for finding and comparing terms across statutes and helps demonstrate the comparability and similarity of obligations (rather than dissimilarities) across jurisdictions.
APPENDIX 9: PRIVACY TOOLKIT TEMPLATES

TABLE OF CONTENTS as of July, 2006

These templates are actual policies and procedures in use by various organizations across Canada. They are listed in alphabetical order by policy. This table also shows the contributing organization and identifies the possible (not exclusive) elements that the policy/procedure may address.

NOTE: When using one of these templates, please acknowledge the contributing Site.

<table>
<thead>
<tr>
<th>POLICY - PROCEDURE FOR USE AS A TEMPLATE</th>
<th>ELEMENT(S)</th>
<th>SITE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Policy - Research Uses of Linked Data</td>
<td>1, 7, 8, 9</td>
<td>CHSPR</td>
</tr>
<tr>
<td>Access - Disclosure and Corrections to Clinical Record under Mental Health Act Policy 10.40.050</td>
<td>1,7,8,9</td>
<td>WRHA</td>
</tr>
<tr>
<td>Access to Personal Health Information Policy 10.40.040</td>
<td>1,7,8,9</td>
<td>WRHA</td>
</tr>
<tr>
<td>Access, Security and Confidentiality Policy</td>
<td>1, 7, 8, 9</td>
<td>MCHP</td>
</tr>
<tr>
<td>Audit of Security Safeguards Policy Policy 10.40.060</td>
<td>7</td>
<td>WRHA</td>
</tr>
<tr>
<td>Certificate of Destruction/Undertaking</td>
<td>7, 9</td>
<td>WSIB</td>
</tr>
<tr>
<td>Cessation of Staff Employment/Appointment - Exit Form</td>
<td>10</td>
<td>MCHP</td>
</tr>
<tr>
<td>Client Information Request Form for Aggregate Data (doc)</td>
<td>2, 8</td>
<td>CIHI</td>
</tr>
<tr>
<td>Client Information Request Form for Aggregate Data (pdf)</td>
<td>2, 8</td>
<td>CIHI</td>
</tr>
<tr>
<td>Client Information Request Form for Record-Level Data (doc)</td>
<td>1, 2, 8</td>
<td>CIHI</td>
</tr>
<tr>
<td>Client Information Request Form for Record-Level Data (pdf)</td>
<td>1, 2, 8</td>
<td>CIHI</td>
</tr>
<tr>
<td>Collection of PHI - Restrictions and Notice Requirements policy 10.40.070</td>
<td>2</td>
<td>WRHA</td>
</tr>
<tr>
<td>Communications and Knowledge Transfer &amp; Exchange Privacy Policy</td>
<td>10</td>
<td>IWH</td>
</tr>
<tr>
<td>Confidential Information Agreement - Researcher</td>
<td>7</td>
<td>MCHP</td>
</tr>
<tr>
<td>Confidentiality - Personal Health Information Policy 10.40.020</td>
<td>7</td>
<td>WRHA</td>
</tr>
<tr>
<td>Confidentiality Agreement – 2005 Version</td>
<td>7</td>
<td>HQC</td>
</tr>
<tr>
<td>Confidentiality Agreement – October 2005</td>
<td>7</td>
<td>ICES</td>
</tr>
<tr>
<td>Confidentiality Contract</td>
<td>7</td>
<td>PHRU</td>
</tr>
<tr>
<td>Data Access Form 20030711v6</td>
<td>1, 7, 8, 9</td>
<td>CHSPR</td>
</tr>
<tr>
<td>Data Access Request Guidelines and Procedures</td>
<td>1, 7, 8, 9</td>
<td>PHRU</td>
</tr>
<tr>
<td>Data Access Request Guidelines and Procedures</td>
<td>1, 7, 8, 9</td>
<td>MCHP</td>
</tr>
<tr>
<td>Data Destruction and Retention Policy</td>
<td>7, 8, 9</td>
<td>MCHP</td>
</tr>
<tr>
<td>Data Destruction Policy and Procedures</td>
<td>7, 8, 9</td>
<td>ICES</td>
</tr>
<tr>
<td>Data Sharing Agreement Template</td>
<td>2, 7, 10</td>
<td>MCHP</td>
</tr>
<tr>
<td>Data Stewards – Terms of Reference</td>
<td>7</td>
<td>CCO</td>
</tr>
<tr>
<td>Data Use and Disclosure Policy</td>
<td>7, 8, 9</td>
<td>CCO</td>
</tr>
<tr>
<td>Definitions Policy 10.40.030</td>
<td>10</td>
<td>WRHA</td>
</tr>
<tr>
<td>Disposal of Confidential Material Including PHI Policy 10.40.090</td>
<td>7, 8, 9</td>
<td>WRHA</td>
</tr>
<tr>
<td>POLICY - PROCEDURE FOR USE AS A TEMPLATE</td>
<td>ELEMENT(S)</td>
<td>SITE</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>Dissemination of Research Findings Policy (includes small cell size limits/suppression requirements)</td>
<td>10</td>
<td>MCHP</td>
</tr>
<tr>
<td>Document Shredding Policy and Procedures</td>
<td>7, 8</td>
<td>ICES</td>
</tr>
<tr>
<td>(REB) Ethics Review Policy and Procedures</td>
<td>1, 8</td>
<td>ICES</td>
</tr>
<tr>
<td>Ethics II Toolkit - FNC</td>
<td>1, 8</td>
<td>NAHO</td>
</tr>
<tr>
<td>Facility Security Policy</td>
<td>7</td>
<td>MCHP</td>
</tr>
<tr>
<td>FIPPA Agreement for the Protection of Personal Information for Research Purposes</td>
<td>1, 2, 8</td>
<td>WRHA</td>
</tr>
<tr>
<td>Guidelines for Student Use of the Population Health Research Data Repository</td>
<td>1, 2, 8</td>
<td>MCHP</td>
</tr>
<tr>
<td>Health Information Policy Committee (HIPC) Request for Access to Health Information</td>
<td>1, 2, 7, 8</td>
<td>MCHP</td>
</tr>
<tr>
<td><a href="http://secure.cihi.ca/cihiweb/dispPage.jsp?cw_page=privacy_e">http://secure.cihi.ca/cihiweb/dispPage.jsp?cw_page=privacy_e</a></td>
<td>1, 2, 7</td>
<td>CIHI</td>
</tr>
<tr>
<td><a href="http://www.iwh.on.ca/about/privacy.php">http://www.iwh.on.ca/about/privacy.php</a></td>
<td>1, 7, 8, 10</td>
<td>IWH</td>
</tr>
<tr>
<td>Human Resources Employee Privacy Policy</td>
<td>10</td>
<td>IWH</td>
</tr>
<tr>
<td>Importing External Data Sets Policy and Procedures</td>
<td>2, 7</td>
<td>ICES</td>
</tr>
<tr>
<td>Information Breach Policy and Procedures</td>
<td>7, 10</td>
<td>ICES</td>
</tr>
<tr>
<td>Information Sharing Agreement</td>
<td>2, 7</td>
<td>CHSPR</td>
</tr>
<tr>
<td>Orientation Checklist</td>
<td>10</td>
<td>MCHP</td>
</tr>
<tr>
<td>Passwords Policy and Procedures</td>
<td>7, 8</td>
<td>ICES</td>
</tr>
<tr>
<td>Passwords Policy rev Oct 2005</td>
<td>7, 8</td>
<td>ICES</td>
</tr>
<tr>
<td>PHIA - Research Agreement for Access to PHI for Research Purposes</td>
<td>1, 2</td>
<td>WRHA</td>
</tr>
<tr>
<td>PHIA in a REB Context</td>
<td>1</td>
<td>WRHA</td>
</tr>
<tr>
<td>Pledge of Privacy - <a href="http://www.umanitoba.ca/centres/mchp/policies_external/privacy.htm">http://www.umanitoba.ca/centres/mchp/policies_external/privacy.htm</a></td>
<td>10</td>
<td>MCHP</td>
</tr>
<tr>
<td>Policies and Procedures for Protecting Privacy of PHI – 10-7-03</td>
<td>1, 2, 7, 8</td>
<td>NFL</td>
</tr>
<tr>
<td>Principles, Guidelines - 2004</td>
<td>7, 8, 10</td>
<td>NFL</td>
</tr>
<tr>
<td>Privacy and Confidentiality of Health Information at CIHI</td>
<td>1, 2, 7, 8</td>
<td>CIHI</td>
</tr>
<tr>
<td>Privacy Breach Policy rev Oct 05</td>
<td>7</td>
<td>ICES</td>
</tr>
<tr>
<td>Privacy Code</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>HQC</td>
</tr>
<tr>
<td>Privacy Code</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>MCHP</td>
</tr>
<tr>
<td>Privacy Code: Protecting Personal Health Information at ICES</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>ICES</td>
</tr>
<tr>
<td>Privacy Impact Assessment (PIA) Abbreviated Form</td>
<td>2</td>
<td>HQC</td>
</tr>
<tr>
<td>Privacy Impact Assessment Form (doc) project specific</td>
<td>1, 2</td>
<td>ICES</td>
</tr>
<tr>
<td>Privacy Impact Assessment Form (pdf) project specific</td>
<td>1, 2</td>
<td>ICES</td>
</tr>
<tr>
<td>Privacy Impact Assessment Report Format</td>
<td>1, 2</td>
<td>WSIB</td>
</tr>
<tr>
<td>Privacy Leads – Terms of Reference</td>
<td>10</td>
<td>CCO</td>
</tr>
<tr>
<td>POLICY - PROCEDURE FOR USE AS A TEMPLATE</td>
<td>ELEMENT(S)</td>
<td>SITE</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------</td>
<td>------</td>
</tr>
<tr>
<td>Privacy Policy</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>CCO</td>
</tr>
<tr>
<td>Privacy Policy</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>NAHO</td>
</tr>
<tr>
<td>Privacy Policy and Procedures 1-04</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>CHSPR</td>
</tr>
<tr>
<td>Privacy Statement, Sept 03 – (Draft)</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>CHSPR</td>
</tr>
<tr>
<td>Privacy Statement for Workers: <a href="http://www.wsib.on.ca/wsib/wsibsite.nsf/public/PrivacyPolicy">http://www.wsib.on.ca/wsib/wsibsite.nsf/public/PrivacyPolicy</a></td>
<td>1, 2, 7, 8, 9, 10</td>
<td>WSIB</td>
</tr>
<tr>
<td>Privacy Toolkit</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>CIHI</td>
</tr>
<tr>
<td>Privacy Toolkit</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>NAHO</td>
</tr>
<tr>
<td>Privacy Tools</td>
<td>1, 2, 7, 8, 9, 10</td>
<td>PEI</td>
</tr>
<tr>
<td>Privacy, Confidentiality and Access Standards – 10-10-03</td>
<td>1, 7, 8</td>
<td>NFL</td>
</tr>
<tr>
<td>Privacy, Confidentiality and Data Security: Handbook of Research Policies and Procedures</td>
<td>1, 7, 8</td>
<td>IWH</td>
</tr>
<tr>
<td>Private Sector Guidelines</td>
<td>2, 8</td>
<td>MCHP</td>
</tr>
<tr>
<td>Protocol for Utilizing the Population Health Research Data Repository</td>
<td>8</td>
<td>MCHP</td>
</tr>
<tr>
<td>Public Brochure 2005</td>
<td>10</td>
<td>ICES</td>
</tr>
<tr>
<td>Research Ethics Board (REB) – Application Form, University of Manitoba</td>
<td>1, 8</td>
<td>MCHP</td>
</tr>
<tr>
<td>Research Agreement</td>
<td>2, 7, 8, 9</td>
<td>ICES</td>
</tr>
<tr>
<td>Research Agreement Form - <a href="http://www.wsib.on.ca/wsib/wsibsite.nsf/public/ethicscode">http://www.wsib.on.ca/wsib/wsibsite.nsf/public/ethicscode</a></td>
<td>2, 7, 8, 9</td>
<td>WSIB</td>
</tr>
<tr>
<td>Researcher Confidential Information Agreement</td>
<td>2, 7, 8, 9</td>
<td>MCHP</td>
</tr>
<tr>
<td>Retention and Destruction of Data Policy 3-1-06</td>
<td>7, 9</td>
<td>MCHP</td>
</tr>
<tr>
<td>Security and Confidentiality Policies and Procedures</td>
<td>2, 7, 10</td>
<td>HQC</td>
</tr>
<tr>
<td>Security and Storage of PHI Policy 10.40.120</td>
<td>2, 7, 10</td>
<td>WRHA</td>
</tr>
<tr>
<td>Security Breaches and Corrective Procedures Policy 10.40.110</td>
<td>7</td>
<td>WRHA</td>
</tr>
<tr>
<td>Shredding Policy</td>
<td>7, 8, 9</td>
<td>ICES</td>
</tr>
<tr>
<td>Surveillance Tool Kit</td>
<td>1, 7, 8, 10</td>
<td>NAHO</td>
</tr>
<tr>
<td>Transmission of PHI via Fax Policy 10.40.130</td>
<td>1, 7, 8</td>
<td>WRHA</td>
</tr>
<tr>
<td>University of Manitoba Policy 216: FIPPA and PHIA - <a href="http://www.umanitoba.ca/admin/governance/policies/section_200/216.shtml">http://www.umanitoba.ca/admin/governance/policies/section_200/216.shtml</a></td>
<td>1, 2, 7, 8, 9, 10</td>
<td>MCHP</td>
</tr>
<tr>
<td>Use and Disclosure of PHI Policy 10.40.100</td>
<td>7, 8, 10</td>
<td>WRHA</td>
</tr>
<tr>
<td>Visitors to ICES Policy and Procedures</td>
<td>1, 7</td>
<td>ICES</td>
</tr>
<tr>
<td>Web FAQ List (Nov 2005)</td>
<td>1, 7, 9, 10</td>
<td>ICES</td>
</tr>
<tr>
<td>Organization</td>
<td>Abbreviation</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>Cancer Care Ontario</td>
<td>CCO</td>
<td></td>
</tr>
<tr>
<td>Centre for Health Services and Policy Research, University of British Columbia</td>
<td>CHSPR</td>
<td></td>
</tr>
<tr>
<td>Canadian Institute for Health Information</td>
<td>CIHI</td>
<td></td>
</tr>
<tr>
<td>Health Quality Council - Sask.</td>
<td>HQC</td>
<td></td>
</tr>
<tr>
<td>Institute for Clinical and Evaluative Sciences, Ontario</td>
<td>ICES</td>
<td></td>
</tr>
<tr>
<td>Institute for Work and Health - Ontario</td>
<td>IWH</td>
<td></td>
</tr>
<tr>
<td>Manitoba Centre for Health Policy, University of Manitoba</td>
<td>MCHP</td>
<td></td>
</tr>
<tr>
<td>National Aboriginal Health Organization</td>
<td>NAHO</td>
<td></td>
</tr>
<tr>
<td>Newfoundland and Labrador Centre for Health Information</td>
<td>NFL</td>
<td></td>
</tr>
<tr>
<td>Prince Edward Island, Department of Health and Social Services</td>
<td>PEI</td>
<td></td>
</tr>
<tr>
<td>Population Health Research Unit, Dalhousie University</td>
<td>PHRU</td>
<td></td>
</tr>
<tr>
<td>Winnipeg Regional Health Authority</td>
<td>WRHA</td>
<td></td>
</tr>
<tr>
<td>Workplace Safety &amp; Insurance Board - Ontario</td>
<td>WSIB</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 10: Input from the Pilot Project (July – October 2006)

At the third workshop, the team asked for volunteers to pilot the draft Privacy Best Practices for Secondary Data Use (SDU) during the summer/early fall of 2006. The team recognized the time limitations that this might exert because of grant writing and vacations, and thank colleagues who were able to provide input.

The sites that participated in the pilot include NFLD & Labrador Centre for Health Information, Saskatchewan Health Quality Council, The Integrated Health Care and Research Network of Quebec, Cancer Care Ontario and the Institute for Work and Health in Toronto.

Sharing of approaches to privacy policies and procedures among some Canadian research organizations has provided some insight into data issues successfully resolved in these jurisdictions individually. This sharing of activities has served to improve and harmonize data protection practices across these organizations, as well as saving time and expense. Knowing specifically how privacy issues are being handled by other organizations and learning from their practical experiences helps stimulate the development of privacy best practices for other organizations grappling with the same issues.

Different research organizations have engaged in this collaborative process at different periods.

- Some of the institutes which were part of the collaborative team had previous experience in sharing templates to create policies and practices, which was the genesis of this project (MCHP and ICES, 1997 – 2004);
- Other institutes had contacted privacy and data security staffers at these sites and asked if it was possible to review in-house templates of privacy/data security policies and other documents (i.e., PHRU, 2004) with the mutually-agreed upon intent to compare and borrow as possible;
- A new organization made site visits to ICES and MCHP to explicitly review data security and privacy protections as well as seek help with building appropriate policies, practices and standards for their jurisdiction using the template approach (Saskatchewan HQC, 2003).
- In 2006, the newly-named Privacy Officer /Scientist at HQC, piloted the privacy best practices using the checklist to “guide a logical process to ensure that a research project (and research environment) is developed to adhere to privacy best practices”.
- Established organizations with extensive privacy compliance programs (i.e., CCO) reviewed the privacy best practices for SDU in concert with their annual update of policies and procedures.
- One organization with extensive privacy/data security practices and policies

Here are some of the findings from these different organizations about the Privacy Best Practices for SDU pilot documents. We have purposefully left out the mechanical,
formatting and proofreading suggestions (which were by and large incorporated as recommended).

Pamela Spencer, VP Corporate Affairs, General Counsel & CPO
Melissa Hudson, Associate Privacy Officer
Cancer Care Ontario, Toronto, ON

“…While Cancer Care Ontario has an extensive Privacy Compliance Program in place, we found the SDU documents essential to our annual update of privacy policies and procedures this fall. In this regard, we found the “Checklist” and its free-form reporting format particularly helpful.

The holistic approach to privacy for SDU – including statutory authorities and best-practices – is very effective…allowed us to evaluate both the “floor” (i.e. statutes) and the “ceiling” (i.e. best-practices) of privacy compliance practices, and to ensure that CCO strives to meet the latter. The cross-provincial make-up of the pilot documents also provides a valuable educational tool and will allow us to discuss privacy practices in a coherent fashion with stakeholders throughout Canada.

The SDU Privacy Toolkit is comprehensive in scope and allowed us to easily and effectively chart our privacy-related strengths and opportunities for increased compliance. The Dictionary, “Rules-in-a-Box” and the Encyclopaedia are excellent reference materials and form an effective foundation for the SDU pilot documents. The templates are exhaustive and helpful, although we would suggest more descriptive labeling and an improved organizational structure.

Our overall perception is that this process was well-conceived and executed and that our most valuable contributions may lie in providing possible “next-steps”, or areas for further development. As an exercise in “due diligence”, the Privacy Best Practices for SDU forms an excellent foundation; in the future, we suggest an analysis of the following:

(1) Implementation: how to translate these principles into effective practice; for example, privacy orientation and training – what works and why? How to create a “culture of privacy” How to measure employee compliance in a meaningful fashion?

(2) Communication and Transparency: How to communicate effectively with stakeholders on privacy related matters; for example, patients, primary data collectors, privacy commissioners, government ministries, and the media.

(3) The Relationship between Privacy and Security: What are the key complementarities? How and when should they be integrated? The interaction of policy and technology, etc.
(4) **Quantifying Risk**: How to prioritize risk and response in a world of limited resources; e.g. the role of human error vs. technological failure, etc.

(5) “**Risky Relationships**”: How to ensure that consultants / agents / third-party service providers provide comparable levels of privacy / security. How to effectively monitor third-parties, etc.

(6) **Auditing**: The role of the external privacy consultant. When is an external consultant necessary? How to facilitate this role?

We look forward to seeing the final documents.

---

**Sheilah Hogg-Johnson PhD, Senior Scientist, Manager and Privacy Officer**  
**Institute for Work and Health, Toronto ON**

“Congratulations on distilling and organizing such a vast amount of work and information. The team that worked to assemble all this has done an excellent job and the materials clearly reflect the work done at the workshops and behind the scenes to prepare for the workshops. The materials are well organized into sections. I appreciate the alignment with the CIHR Best Practices to allow cross-referencing. I also found it very helpful to have the reference materials (encyclopedia, the “rules in a box” and the dictionary particularly) to refer to as necessary.

“…Might you consider adding a very brief section to help navigate the materials – perhaps bullet points or a flowchart near the very beginning called “How to use these materials” or “Roadmap to the materials”?

For our review at IWH, my plan is to have the binder of Pilot Documents on hand and to work through the document called “Checklist” in conjunction with the section “Privacy Best Practices for Secondary Data Use” pages 5-12. I will do this with the IWH Privacy Committee, with all our materials also assembled and at hand.”

**Dr. Gillian Bartlett-Esquiland, McGill University, Clinical Health and Informatics Research in Montreal**

“I found the documents very useful - particularly the templates. One of the things I think this will be the most helpful for is cross-province or linked multi-province studies as it gives the national perspective on the privacy legislation. Also, it helps for planning when putting together grants.”

The templates index:
“...It would be very helpful to have this list in two additional formats. This would mean keeping the current list but also having a list that is alphabetized by the donating organization and a third list where the templates are grouped by type of document (i.e. all confidentiality agreements put together).”

The checklist index:
“...Some of the elements work very well if you are the researcher but I found them less helpful or pertinent as a data steward, custodian or gatekeeper (i.e. 2.2, 2.3 and 7.4; 7.1, 7.3 and 7.5; 7.6 and 7.8). You may want to divide the checklist into two - one for researchers and another for someone releasing information (data steward, custodian etc).”

“I believe these sections were more recent additions but very useful. Please let me know when the final document will be available as I have many people I wish to send a copy!!”

Alex Agnew, then Director of Corporate Services, Saskatchewan Health Quality Council wrote to us about his experience back to 2003 with the inception of HQC:

“there were benefits in this approach of using templates that these organizations had developed and used in their day-to-day activities, including:
- The opportunity to work with agencies that have been in operation for many years – and had therefore established solid processes regarding the use of personal health information – was very beneficial to the HQC.
- Considerable costs savings were achieved from working in this fashion.
- More importantly, it allowed HQC to have proven and credible processes in place in a much shorter period of time.”

Dr. Gary Teare, Director, Quality Measurement and Analysis, Saskatchewan Health Quality Council updated that experience with these comments in Oct 2006:

“a pleasure to test-run the…SDU pilot documents. I have found them extremely useful – particularly since I have recently taken on the role of Privacy Officer here at HQC. I found the Checklist and Privacy Best Practices documents particularly helpful… I worked through the Checklist with respect to the SDU projects we have conducted here at the HQC during the past 2 years and identified issues that I needed to follow up on in relation to most of the Elements…there were other areas/issues where the Checklist pointed out gaps in our practices that need to be addressed. This actually provides me with a useful “to do” list for my first months as Privacy Officer!”

“...we need our oversight authorities to clarify for us whether in fact the de-identified data we use here at HQC is in fact considered “de-identified” according to our HIPA legislation (and thus our use of it is exempt from HIPA). We have
always acted and treated the data as if it is subject to HIPA – and it is my understanding that it is. However, the University of Saskatchewan Research Ethics Board has consistently exempted our projects from review because they consider them to be “secondary analysis of de-identified data” – and thus exempt from REB purview according to the Tri-Council guidelines. I’m now thinking that we need to get a clear statement from government lawyers and from the Privacy Commissioner as to whether the data we use (especially because we do a lot of linkage) is really not exempted from HIPA by the exemption for research using only “de-identified” data. Then, if it is clarified that it is not exempt from HIPA, we need to insist that the U of S REB at least do an expedited review of the research proposals that we submit to them”

“The Privacy Best Practices document was very helpful – as this provided the link between the elements and the resources/tools that are included in the package. My suggestion to make this resource even more user-friendly would be to organize the tools in the “Templates” directory on the CD-ROM into folders by “type” of tool/policy… it would also help the user-friendliness of these extensive materials if the different documents had some distinguishing visual clue to help the reader know immediately which document he/she is looking at when looking at any page”.

“This toolkit will prove to be a really valuable resource for privacy officers, researchers and REBs. I’ve already alerted the new Privacy Officer at Saskatchewan Health…that this resource will be available soon. She didn’t know about the project – and I think she will find it useful to her work as well. Congratulations on a job well done”.

Dr. Lucy McDonald, Director of Communications & Privacy, Newfoundland & Labrador Centre for Health Information, St. John's, NL

“I want to congratulate you on developing a very useful document. I feel that this document is well written and well organized. At this time I have a few comments and suggestions that I will outline below:

- Include a backgrounder to indicate the increasing relevance of secondary data use and the implications that it may have on privacy. I believe that this would provide further background on the need for a toolkit or best practices to harmonize privacy and research for those who have been asked to develop polices but are not clear on the overarching/driving purpose.
- I feel that there are many inconsistent methods for determining the "reasonable limits" on retention. Data holders vs. researcher vs. REB may have quite different policies and procedures around retention. Although this may be beyond the scope of this document, I would like to see one approach that has been used to harmonize retention practices in an acceptable manner to all parties.
- As a follow-up to these Pilot Documents, I would suggest that the Core Team for the Harmonizing Privacy and Research Initiatives provide two documents across
Harmonizing Research & Privacy: Standards for a Collaborative Future.
Privacy Best Practices for Secondary Data Use (SDU)

Canada…one document… aimed at data custodians/ those who release data for secondary data purposes; the other aimed at researchers who wish to use data for a secondary research purpose. Each...should be aligned, whereby a researcher would know they are implementing privacy practices that are in line with the requirements set by the custodian.

- As well, these two documents should reference the Available Toolkit templates and have an online resource centre to easily retrieve the needed documents…
- In terms of dissemination, it would be useful if the 'Privacy Best Practices for Secondary Data Use' toolkit could be available for Privacy Commissioners, REBs and custodians across Canada.

Again, thank you for the opportunity for involvement in this effort to harmonize privacy and research, particularly for secondary data use. I look forward to working more with this document, by way of implementation and appropriate dissemination”.