



Striking a Balance: Facilitating Access to Patient Safety Data While Protecting Privacy Through Creation of a National Harmonized Standard

July 2007

Investigators:

Karen Weisbaum, LLB MA, Queen's University
Sylvia Hyland, Institute for Safe Medication Practices Canada (ISMP Canada)
Eleanor Morton, Healthcare Insurance Reciprocal of Canada (HIROC)

Table of Contents

Acknowledgement	3
Main Messages	4
Executive Summary	6
Context	12
Implications	14
Approach, Methodology, Rationale, Assumptions	16
Results, Conclusions	19
Recommendations	45
References	59

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

Acknowledgement

This research project was funded in part through research funding from the Canadian Patient Safety Institute (CPSI) and through in-kind contributions from the home institutions of each coauthor: Queen's University and Biotika Inc., Montréal (K. Weisbaum), Institute for Safe Medication Practices Canada (S. Hyland), and the Healthcare Insurance Reciprocal of Canada (HIROC) (E. Morton.)

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

Main Messages

Background and Purpose

In its report entitled *Building a Safer System: A National Integrated Strategy for Improving Patient Safety in Canadian Health Care* (2002) (the Report), the National Steering Committee on Patient Safety recommended that privacy legislation be standardized in order to balance the need for access to patient safety data and the requirement to respect the privacy of patients and providers. Knowing that standardization of privacy legislation and other relevant and applicable statutes is not likely, but that some sort of national harmonized policy, grounded in a review of privacy legislation, plus accompanying “best practices” for handling patient safety data in a privacy-protective manner, might be a possible alternative, the original purpose of this report/project was to explore the feasibility and utility of a harmonized national policy. We purposefully decided to limit our scope to consideration of patient safety data that is also medication incident data. We used the term “sharing” in reference to external incident reporting that is voluntary. Our overall findings were as follows:

- 1. Incident information that is both non-identifying and factual is also sharable information.** Limits on sharing information that stem from privacy rules and other types of confidentiality provisions that apply to statutorily protected information (for example, through evidentiary privilege) are not necessarily applicable to incident data. What counts for determining if sharing is permitted are the characteristics of the data themselves. At least in the case of medication incident data, sharing will be greatly facilitated through *harmonization of those characteristics* according to an accepted standard or format, and the

fact that privacy standards are not harmonized—or are perceived as not harmonized—will not present a barrier to sharing.

2. **The Saskatchewan Critical Incident Reporting Guideline includes categories of incidents that might serve as an interesting potential template/model** for conceptualizing and organizing incident information into functional categories for other systems of incident reporting.
3. **Consideration of statutory harm reduction provisions should inform ongoing discussion of the need for balancing privacy with incident information sharing.** Statutory privacy protections are always on balance with public welfare and safety, and appeals to privacy entitlements should not necessarily override serious risks of harm. Some statutory provisions permit disclosure of identifying information under specific circumstances, and should be considered when constructing policy arguments about such balancing.
4. **From an ethics perspective, there are benefits to being transparent when it comes to incident information sharing.** Where rules regarding identifiability of information and privilege do not apply, it may be difficult from an *ethical* perspective to justify placing limits on sharing of incident data, in particular, where the benefits of sharing have been demonstrated, for example, the US-based Manufacturer and User Facility Device Experience Database (MAUDE.)

Executive Summary

Background and Purpose

In its 2002 report entitled *Building a Safer System: A National Integrated Strategy for Improving Patient Safety in Canadian Health Care*¹, the National Steering Committee on Patient Safety recommended that privacy legislation be standardized as a way to balance the need for access to patient safety data with the requirement to respect the privacy of both patients and providers. Standardization of privacy legislation and other relevant and applicable statutes is unlikely; however, some sort of harmonized national policy and accompanying “best practices” for handling patient safety data in a privacy protective manner might be a reasonable alternative goal. Therefore, the original purpose of the project described in the current report was to explore the feasibility and utility of such a harmonized policy. A scan of pertinent legislation appeared to be one way of finding privacy rules that are common across statutes and that could be used as a foundation for developing policy. We purposely limited our scope to consideration of patient safety data that also function as medication incident data. The term “medication incident” is widely used to represent the preventable subset of potential and actual adverse drug events. We focused on the statutory limits and permissions that apply to external reporting (i.e., disclosures of incident data by entities governed by statute [such as hospitals and regulated health professionals] to parties other than the institution or entity where the incident occurred). We used the term “sharing” to refer to external incident reporting that is voluntary. Our overall findings are summarized here.

¹ The complete report can be found at http://rcpsc.medical.org/publications/building_a_safer_system_e.pdf

Information that is both non-identifying and factual is also sharable information

In the course of this work, we found that limits on the sharing of incident information stem from a variety of sources, including at least two types of statutory provisions: those limiting the sharing of information that identifies individuals (“personal information”, which, by statutory definition, is also information that identifies individuals, i.e. “identifying information”) and those limiting the sharing of opinions from professionals about the nature of an incident (e.g., in situations where there is evidentiary privilege). However, medication incident information is both non-identifying (rather than personal information) and factual (rather than an opinion about the facts), so it is not caught by many of the statutory privacy rules that are often perceived as applicable. Our findings may have broader implications in the patient safety field: although we examined privacy and related legislation as it pertains to medication incident data, similar dilemmas arise in relation to other sorts of incidents and errors that involve *identifying* information. For this reason, and also because others may disagree about the non-identifiable nature of medication incident information, we also reviewed the rules set out in statutes applying to the handling and sharing of “protected information” and attempted to garner additional insights into the significance of such provisions.

In short, we found that limits on the sharing of incident information that stem from privacy rules and other types of confidentiality provisions applying to statutorily protected information (for example, through evidentiary privilege) are not necessarily applicable to incident data. What counts for determining if sharing is permitted are the characteristics of the data themselves. At least in the case of medication incident data, sharing will be greatly facilitated through harmonization of those characteristics according to an accepted standard or format; the fact that

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

privacy standards are not harmonized—or are perceived as not harmonized—will not present a barrier to sharing.

Nevertheless, we believe that the scope of the statutory limits discussed above have occasionally been misinterpreted as overly broad. As a result, the limits on the sharing of incident data—particularly, in our experience, medication incident data—have sometimes been misunderstood. Given that effective incident data are (or can be) factual, and given that such data meet all tests for being non-identifiable, what is really needed is a set of nationally accepted categories of data elements to be used for reporting medication incidents (and indeed all types of incidents) across Canada.

The need for standardized categories—a Saskatchewan example

The collection of data according to a single “standard” would overcome privacy and other confidentiality concerns, provided that the categories are used consistently by all persons and organizations collecting and using incident data and provided that all such data are foreseeably both non-identifying and factual. In this regard, the categories of incidents in the Saskatchewan Critical Incident Reporting Guideline might serve as a template or model for conceptualizing and organizing incident information into functional categories for other systems of incident reporting. Establishing and standardizing similar lists for other categories and subcategories of incidents, particularly if the data elements in each category could be grouped for application of tests for de-identification, might make it easier to comply with statutory rules in determining whether, or to what extent, sharing is permissible.

Role of statutory harm-reduction provisions

The main goals of privacy statutes are to protect individuals' personal privacy and to uphold requirements for confidentiality. Yet the protection of privacy was never intended to trump all other claims. Rather, the requirement for privacy must be balanced against public welfare and safety, and appeals to privacy entitlements should not necessarily override serious concerns about potential harm. Some statutory provisions permit disclosure of identifying information under specific circumstances, which may or may not apply to flows of incident information. Although we do not conclusively argue for or against the claim that such provisions may be applicable to incident reporting, we mention these provisions as examples of existing statutory “clues” to the justification of the need for balancing, where identifying information is being shared. Consideration of such provisions may provide a basis for policy arguments that the rationales behind existing provisions must logically apply to flows of incident information (possibly of any type) that identifies or that may identify individuals.

Ethics and the benefits of transparency

Where rules regarding the identifiability of information and privilege do not apply, it may be difficult from an ethics perspective to justify placing limits on the sharing of incident data, in particular where the benefits of sharing have already been demonstrated. Such is the case with the US-based Manufacturer and User Facility Device Experience Database (MAUDE), a non-Canadian example demonstrating that events can be shared openly as a way to facilitate learning. MAUDE, the best available model internationally, sets a precedent for transparency.

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

Summary of Categories of Information

Category	Rule for disclosure or sharing for the purpose of incident reporting
1. Information that is not identifiable (i.e., not defined under a statute as personal information [PI] or personal health information [PHI]) and is not protected information (i.e., is factual information)	This category of information can be disclosed/shared for the purpose of incident reporting.
2. Information that is identifiable (i.e., is PI or PHI), for which the patient and/or a surrogate has provided consent to disclose	This category of information can be disclosed/shared for the purpose of incident reporting.
3. Information that is identifiable (i.e., is PI or PHI), but the exceptional circumstances of the incident meet a test of a harm-reduction provision that is set out in a key statute	This category of information can be disclosed/shared for the purpose of incident reporting.
4. Information that is not identifiable (i.e., is not PI or PHI), but is protected information	This category of information cannot be disclosed/shared for the purpose of incident reporting.
5. Information that is not identifiable (i.e., is not PI or PHI), but is protected information and there are exceptional circumstances that meet a test of a harm-reduction provision set out in a key statute	This category of information can be disclosed/shared for the purpose of incident reporting.
6. Information that is identifiable (i.e., is PI or PHI), is protected information, or both, but to which an exception applies (i.e., in the scope of this report, it would be a statutory exception, for example, where reporting is required by law or permitted by a special statute)	This category of information can be disclosed/shared for the purpose of incident reporting.
7. Information that is identifiable (i.e., is PI or PHI) and there is no exception, no consent, and no circumstances that meet a harm-reduction provision	This category of information cannot be disclosed/shared for the purpose of incident reporting.

Conclusions

We conclude that the sharing of medication incident information requires information that is both non-identifying and factual. While organizations must comply with the legislative rules in their own jurisdictions, general rules related to the privacy of personal information mean that medication incident information falls outside the application of statutory privacy rules. This is not necessarily the case for other types of incident data, but there is a strong argument to be made that statutory rules, in principle, support the sharing of information where the goal is to protect the safety of patients. The benefits of medication incident reporting and learning systems have been eloquently outlined in a World Health Organization report. It is our considered

This project is partially funded by:



Striking a Balance: Facilitating Access to Patient Safety Data While Protecting Privacy Through Creation of a National Harmonized Standard

Investigators:
Weisbaum et al., 2007

opinion that, in all the jurisdictions in Canada, the general rules related to privacy of personal and personal health information and of quality-assurance-related opinions mean that *non-identifying facts* about an incident *are* sharable. We hope that the results of our study will aid health care practitioners and health service organizations in reassuring themselves about sharing of important information about preventable adverse drug events.

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

Context

In its 2002 report entitled *Building a Safer System: A National Integrated Strategy for Improving Patient Safety in Canadian Health Care*,² (hereafter referred to as the patient safety report), the National Steering Committee on Patient Safety recommended that privacy legislation be standardized as a way to balance the need for access to patient safety data with the requirement to respect the privacy of both patients and providers.

Most provinces and territories have had privacy legislation of some type in place for a number of years. Certain privacy statutes are specific to health information, with some of these coming into force only after publication of the patient safety report in 2002. All of the privacy statutes govern the handling of personal information by various kinds of persons or organizations. In general, the statutes have in common the same framework of 10 fair information practices—also known as the 10 “privacy principles”—on which the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) is based.³ Across Canada, hospitals, healthcare professionals, and other organizations that handle personal health information have in place (or should have in place) privacy policies, structured according to these 10 privacy principles, to guide their handling of personal health information and to help them comply with provincial statutory requirements.

Nevertheless, privacy legislation is not—nor is it ever likely to be—standardized. For example, there are subtle differences in the way that definitions are structured, such that what constitutes “personal information” or “personal health information” may differ slightly from one statute to another. The circumstances under which personal or personal health information can be collected without consent also differ. In short, in the absence of standardized legislation, hospitals and

healthcare professionals have understandable concerns about sharing information, such as patients’ personal health information and patient safety data.

In addition, legislation applicable to the sharing of patient safety data is not always limited to privacy statutes. Most privacy legislation applies to information that identifies an individual or information that might be used in a way that could lead to such identification. However, not all safety data are necessarily identifiable, nor do they have the potential to be used in identifying individuals. Nevertheless, there may be statutory restrictions on the sharing of such information that generate other kinds of duties of confidentiality: Thus, even though a certain piece of information is not about a particular person, it may nevertheless be confidential.

As noted earlier, standardization of privacy legislation and other relevant statutes across the country is unlikely. The process of generating an individual statute for one jurisdiction can be a mammoth task, let alone producing harmonized legislation across all provinces and territories. However—and in response to the report of the National Steering Committee on Patient Safety—we set out to examine the feasibility of developing a harmonized national policy, a set of “best practices” for handling patient safety data in a privacy-protective manner, based on a review of applicable privacy legislation from across Canada. We hypothesized that from such a legislative scan we might glean the rules that are common across statutes that could be used as part of a foundation for developing policy.

This approach has been explored in other contexts. For example, as discussed in the report entitled “Harmonizing Research and Privacy: Standards for a Collaborative Future”,⁴ Slaughter et al. (2004) considered a similar dilemma in the context of research involving secondary use of population and administrative databases. These authors noted that, in the absence of “identical

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

and seamless privacy legislation across the country, there needs to be some sort of acceptable, interoperable voluntary standard” or policy to which organizations that handle personal information for similar purposes can comfortably subscribe.

To the extent that patient safety data are subject to privacy legislation, a national, voluntary policy for handling such data would facilitate due diligence on the part of the hospitals and healthcare professionals who report medication incidents and the organizations that collect those reports to educate others and to prevent future incidents.

Implications

The original purpose of the project described in this report was to explore the feasibility and utility of a harmonized national policy on the privacy of information related to patient safety. *We purposefully limited the scope of the project to consideration of patient safety data that also function as medication incident data.* A “medication incident” is defined as follows:

Any preventable event that may cause or lead to inappropriate medication use or patient harm while the medication is in the control of the health-care professional, patient, or consumer. Medication incidents may be related to professional practice, drug products, procedures, and systems, and include prescribing, order communication, product labelling/ packaging/ nomenclature, compounding, dispensing, distribution, administration, education, monitoring, and use.⁵

The term “medication incident” is widely used to represent the preventable subset of potential and actual adverse drug events. This term is also recognized as an alternative for the term “medication error”.⁶

We also decided to focus on incident-reporting activities that constitute disclosures, rather than on activities that use incident data. In other words, we have distinguished between in-house incident reporting (a “use” of incident data) and external incident reporting (a “disclosure” of incident data.) In addition, we focused specifically on the statutory limits and permissions that apply to external reporting (i.e., disclosures of incident data by entities that are governed by statute [which may include both hospitals and regulated health professionals] to parties other than the institution or entity where the incident occurred. Because the term “disclosure” can have a different meaning in the clinical setting (where it often refers to telling a patient that an error has occurred in some aspect of his or her care, a topic not addressed in this paper), we used the term “sharing” to refer to external incident reporting that is voluntary.

In the course of our work on this project, we found that limits on the sharing of incident information stem from a variety of sources, including at least two types of statutory provisions: those limiting the sharing of information that identifies individuals (“personal information”, which, by statutory definition, is also information that identifies individuals, i.e., “identifying information”) and those limiting the sharing of opinions from professionals about the nature of an incident (e.g., in situations where there is evidentiary privilege). However, because medication incident information is (as we will argue) both non-identifying (rather than personal information) and factual (rather than an opinion about the facts of an incident), it is highly “sharable” and is not caught by many of the statutory privacy rules that are often perceived as applicable.

Although the project reported here was specific to medication safety, our findings may have broader implications in the patient safety field: we sought to examine provincial and territorial

privacy legislation and related statutes as they relate to medication incident data, but similar dilemmas arise in relation to other sorts of incidents and errors that involve *identifying* information. For this reason, and also because others may disagree about the non-identifiable nature of medication incident information, we also reviewed the rules set out in statutes applying to the sharing of “protected information” and attempted to garner additional insights into the significance of such provisions.

In short, we found that limits on the sharing of incident information that stem from privacy rules and other types of confidentiality provisions are not necessarily applicable to medication incident data. As discussed in detail in part IV of this report, what counts for determining whether sharing is permitted are the characteristics of the data themselves. At least in the case of medication incident data, sharing will be greatly facilitated through *harmonization of those characteristics* according to an accepted standard or format; the fact that privacy standards are not harmonized—or are perceived as not harmonized—will not present a barrier to sharing.

Approach, Methodology, Rationale, Assumptions

The bulk of the work for this project started with a review of relevant provincial and territorial legislation and associated regulations to identify and then examine the various statutory rules for handling personal or personal health information that are in effect across the country. It quickly became apparent that other statutory materials containing different kinds of confidentiality provisions (the nature of which will become evident in the discussion below) were also relevant to our enquiry. A review of these other materials made it clear that the scope and possibly some key characteristics of the project had already expanded beyond what had been contemplated in the original proposal, and the focus of the work shifted in interesting ways.

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

Literature review

In 2004, Baker et al.⁷ reported an adverse event rate of 7.5% in acute care hospitals in Canada. Of these adverse events, 36.9% were considered *preventable*. These authors estimated, through extrapolation of their study data, that of the almost 2.5 million hospital admissions in Canada in the year 2000, about 185 000 had been associated with an adverse event, and of these, close to 70 000 were potentially preventable.

The Institute of Medicine report *To Err is Human*⁸ recommended voluntary error reporting and collaborative approaches to safety efforts across healthcare organizations. Baker and Norton⁹ also recommended changing legislation to enhance the reporting of errors and near-misses.

One potential barrier to the sharing of patient safety data is the degree of discoverability of patient safety information. Lack of legal protection from discoverability will limit the sharing of patient safety data. This issue has already been debated in the literature. Suydam et al.¹⁰ and Liang et al.¹¹ considered this barrier and suggested that legislation is needed to afford clear and comprehensive nationwide protection to allow the sharing of safety information. Phillips et al.¹² discussed the lack of legal protection from discoverability and the need for enhanced protection to establish effective reporting and to develop a national patient safety database of de-identified data.

Gilmour¹³ has recommended reforming the medical liability system in Canada to reflect the realities of the Canadian federation (such as jurisdiction over tort law, provincially based aspects of healthcare, and questions of how best to create synergies between public and private law to achieve desired goals), to allow the collection of more information about errors, to facilitate systemic analysis of such errors, and to allow implementation of systemic solutions to reduce

future harm. This author provided recommendations for limited qualified privilege legislation for external reporting programs and provisions for systematic identification and dissemination of patient safety lessons learned through structures of provincial patient safety organizations.

Study limitations

For our review of relevant statutes, we had specific questions and issues in mind. We sought to examine rules that might be directly or indirectly applicable to the sharing of medication incident data. Our specific goal was to look for guidance in the privacy statutes (and in a limited number of other kinds of legislation) about what sorts of policy rules could be developed and applied to facilitate sharing, as well as to ensure that any sharing activities would comply with the local legislative rules in each jurisdiction.

By setting these types of limits, our intention was to maintain a manageable research project that could be completed within the time and resources we had available. We hope to elaborate on the findings of this initial project in the future and to expand the scope of application of our results.

It is *essential* that readers reviewing the results reported here keep in mind the narrow agenda of our work: to examine legislation in order to identify issues and promote discussion on our topic.

Our results do not offer, nor were they ever intended to offer, a complete and exhaustive review of all laws relevant to this topic. That is not the nature of this project. Any readers who consider the same statutory materials, particularly if it is for any other purpose and not related to medication incident information, must entail their own review of the original and up-to-date legislation and associated regulations, as well as other materials relevant to their own project and goals.

Results, Conclusions

Summaries of provincial statutory landscapes for reporting incident information

This section summarizes analyses of the key statutes for each province and territory that were reviewed for this paper. Each summary focuses narrowly on statutory rules that can be interpreted as governing disclosures of incident information by the types of organizations or entities to which the statutes apply. Most often, these organizations and entities include hospitals and, in many instances, regulated health professionals.

As discussed later in this report, the definitions of personal information and personal health information are key to determining whether or not a privacy-oriented statute applies to a particular data-handling activity. Readers are cautioned to avoid using the analyses in this section for any purpose beyond the one intended.

Not all types of legislation are discussed in each provincial or territorial summary, since certain types of statutes may be relevant to the analysis in some jurisdictions but not others. For example, in some jurisdictions, statutes applicable to public hospitals contain provisions relevant to the analyses in this report, whereas in other jurisdictions, similar legislation does not include relevant provisions. For ease of reading and reference, the citations for all statutes considered is included at the end of this paper.

British Columbia

Three statutes for British Columbia were considered: the *Freedom of Information and Protection of Privacy Act* (FIPPA), the *Evidence Act*¹⁴, and the *Personal Information Protection Act*¹⁵ (PIPA).

The rules in FIPPA apply to the handling of personal information by entities covered by the legislation, including disclosure of identifiable personal information by, for example, hospitals. Such disclosures can be made for a particular purpose as set out in the Act or with the valid consent of the individual concerned. FIPPA also contains a mandatory override of all of its other sections (a type of provision referred to in this report as a “harm-reduction provision”), which provides for disclosure, “without delay”, of information about “a risk of significant harm”, including harm to the health or safety of the public or a group of people, where disclosure of the information is “clearly in the public interest”.

PIPA sets out how British Columbia organizations (typically those not covered by FIPPA), including corporations, sole proprietorships, partnerships, and nonprofit organizations, may collect, use, and disclose personal information about individuals. This legislation applies to private physicians’ offices. Its core principle is that personal information about patients should not be collected, used, or disclosed without the prior knowledge and consent of those patients, subject to limited exceptions (for example, where disclosure is necessary for medical treatment and the patient does not have the legal capacity to provide consent.)¹⁶

PIPA also contains a harm-reduction provision. Specifically, an organization that is covered by PIPA may not disclose personal information about an individual without the individual’s consent, except if “there are reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual and if notice of disclosure is mailed to the last known address of the individual to whom the personal information relates”.

The *Evidence Act* attaches a special kind of confidentiality to information that is used by a “committee”, as defined in the Act. Such entities would include a hospital committee established

to study, investigate, or evaluate hospital practice or professional care. The limits imposed by the *Evidence Act* include restrictions on records submitted to or compiled by a committee, transcripts of proceedings, and reports or summaries of committee findings. The confidentiality that applies to committee information—known as “privileged” information—meets a particularly high threshold. The committee must not disclose or publish information or records that have been provided to it, except in limited circumstances. Even a witness in a legal proceeding may not be asked or permitted to produce a record that was used by a committee. However, these limits on disclosure of committee information do not apply to original medical or hospital records concerning a patient or to copies of those original medical or hospital records.¹⁷

Alberta

Two Alberta statutes were reviewed: the *Health Information Act*¹⁸ (HIA) and the *Evidence Act*¹⁹. The HIA establishes rules for custodians (entities covered by the Act) that apply to their handling of personal health information, including disclosures by hospitals. The HIA permits disclosure of identifiable personal health information with a patient’s consent. However, unlike most other privacy legislation, the HIA contains an *explicit* exclusion of non identifiable information; as such, disclosure of non-identifiable personal health information is permitted, without consent, for any purpose.

The HIA also explicitly permits disclosure of individually identifying diagnostic, treatment, and care information (which constitutes one kind of personal health information) without the consent of the subject individual in certain situations, including disclosure to a quality assurance committee established under the Alberta *Evidence Act*. A quality assurance committee created by

the Health Quality Council of Alberta would also be considered a quality assurance committee under the provincial *Evidence Act*.

One quality assurance committee may disclose non-identifying health information to another quality assurance committee, but it may not disclose the individually identifying diagnostic, treatment, and care information that it received for its own purposes, as such information is protected. However, the Alberta *Evidence Act* specifically exempts from these protections any original medical and hospital records pertaining to a patient.

The HIA also contains a harm-reduction provision that permits disclosure of personal health information if the disclosure will avert or minimize an imminent danger to the health or safety of any person.

Saskatchewan

The following materials were reviewed for Saskatchewan: the *Regional Health Services Act*²⁰ (RHSA), the Critical Incident Regulations²¹, the Saskatchewan Critical Incident Reporting Guideline, the Saskatchewan *Health Information Protection Act*²² (HIPA), and the *Evidence Act*²³.

The HIPA governs “trustees” that have custody or control of personal health information.

Such trustees include hospitals and regulated health professionals.

The HIPA does not apply to statistical information or to de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to allow the subject individuals to be identified.

The HIPA recognizes the right of an individual (or the individual's substitute decisionmaker) to consent to the use or disclosure of personal health information. Some exceptions to the requirements for consent apply, including disclosure of personal health information to a standards or quality-of-care committee for its established purposes alone, provided that the information is kept confidential. In addition, the provincial *Evidence Act* states that information coming before a hospital's quality assurance committee is privileged. Specifically, a witness in a legal proceeding cannot be asked about, cannot answer questions about, and cannot produce anything with respect to a proceeding before a committee, nor is a report of any kind from such a committee admissible as evidence. There are exceptions to these limits, including the stipulation that these restrictions do not apply to patients' medical and hospital records prepared for the purpose of providing care and treatment in a hospital or prepared as the result of an incident in a hospital (unless the facts of the incident are also fully recorded in the medical or hospital record.) A harm-reduction provision in the HIPA also permits disclosure without consent where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person.

The combination of the RHSA, the Critical Incident Regulations, and the Critical Incident Reporting Guideline create a system of rules that mandate the reporting of critical incidents in Saskatchewan. The Critical Incident Regulations require that notice of a "critical incident" (as defined in the regulations and the guidelines) by a regional health authority to the Minister, or by a healthcare organization to a regional health authority and then on to the Minister, must be given within 3 days of the incident or awareness of the incident. Critical incidents must then be investigated and a written report produced and delivered to the Minister. The content of the

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

report, specified in the regulations, must describe the incident in full.²⁴ The guidelines include a list of 6 categories of events that must be reported to Saskatchewan Health by regional health authorities and healthcare organizations: surgical events (including endoscopy and other invasive procedures), product or device events, patient protection events, care management events, environmental events, and criminal events. Medication incidents appear to fit best within the fourth category, care management events.

However, the regulations stipulate that notices and reports must not include the name of any person to whom the critical incident relates, the name of any healthcare provider involved in providing health services to certain described persons, or anyone operating a program to which the critical incident relates, or the name of any other individual who has knowledge of the critical incident.

Manitoba

The following legislation from Manitoba was considered: the *Personal Health Information Act*²⁵ (PHIA), the *Regional Health Authorities Act*²⁶ (RHAA), and the *Regional Health Authorities Amendment and Manitoba Evidence Amendment Act*²⁷.

The PHIA imposes obligations on trustees for the protection of personal health information, specifically its collection, use, disclosure, and security. The PHIA authorizes trustees to collect personal health information for specific purposes but requires individual consent for use and disclosure, unless an exception applies. The PHIA does not apply to “anonymous” or statistical health information.²⁸

The PHIA applies to trustees who maintain (have custody or control of) personal health information. Under the terms of the PHIA, trustees include licensed or registered health

professionals, healthcare facilities such as hospitals, and health services agencies providing healthcare under an agreement with another trustee.

The requirements of trustees imposed by the PHIA reflect key privacy principles and practices, including the principle that uses and disclosures must be limited to the minimum amount of information necessary to accomplish the particular purpose.

A trustee may disclose personal health information with the subject individual's consent or, in certain circumstances, without their consent. (Some additional limits apply to personal health information numbers.) For example, the PHIA permits disclosure without consent for the purpose of delivering, evaluating, or monitoring a program of the trustee that relates to the provision of healthcare or payment for healthcare, as long as the personal health information disclosed is limited to what the recipient needs to know.

Disclosure without consent is permitted if the disclosure is "to any person if the trustee reasonably believes that the disclosure is necessary to prevent or lessen a serious and immediate threat to that person or to public health or safety"; this constitutes a type of harm-reduction provision.

Part 1 of the *Regional Health Authorities Amendment and Manitoba Evidence Amendment Act* serves to amend the RHAA by adding provisions regarding patient safety.

The *Regional Health Authorities Amendment and Manitoba Evidence Amendment Act* defines the term "critical incident" and imposes on regional health authorities, health corporations, and prescribed healthcare organizations a requirement to establish written procedures respecting information about critical incidents, following minister-approved guidelines. The procedures for recording a critical incident must facilitate prompt creation of a complete record of the incident,

including facts, consequences for the individual, and actions that have been or are to be taken, with prompt notification to the Minister. The regional health authorities, health corporations, and prescribed healthcare organizations involved must jointly strike a critical incident review committee to investigate the incident and the report of the incident and the investigation must be sent to the minister. Incidents that occur within regional health authorities must be handled in a similar fashion.

A committee may require information from persons or entities with custody or control of a document or record—including a record containing personal health information or personal information—relating to the critical incident being investigated and may need to share that information with other committees. However, materials prepared for or by a committee cannot be accessed by anyone, including the subject individuals of incidents. This limit does not apply to a complete record made promptly after the occurrence of the incident, which would include the facts of the incident, its consequences for the individual, and the actions that have been and are to be taken as a result, or to accessing that type of record. However, the limit does not include information about health services provided in an individual's own record of personal health information or information in a record that must be maintained by law.

Part 2 of the *Regional Health Authorities Amendment and Manitoba Evidence Amendment Act* will serve to amend the *Manitoba Evidence Act*. Accordingly, a witness in a legal proceeding cannot be asked and cannot answer questions and cannot make statements about a committee proceeding, and may not produce information (including, without limitation, an opinion or advice) prepared solely for or collected, compiled or prepared by a committee. Notices, reports, other records, and information respecting a critical incident are similarly limited. Records and

information are not admissible as evidence in a legal proceeding. These limits do not apply to information in an individual's health record, to the facts in a record of a critical incident available to the individual affected by the incident (unless those facts are also fully recorded in the individual's record), or to information in a record that is required by law to be created or maintained.

Ontario

The review of Ontario legislation covered the following Acts: the *Personal Health Information Protection Act, 2004*²⁹ (PHIPA) and the *Quality of Care Information Protection Act, 2004*³⁰ (QCIPA).

Ontario's PHIPA governs health information custodians (including healthcare practitioners and hospitals) who handle identifiable personal health information. The statute imposes consent requirements for the collection, use, or disclosure of an individual's personal health information, unless otherwise permitted under its provisions. A health information custodian may disclose (and/or collect and/or use) personal health information about an individual only with consent or as permitted or required by the act, and only if other information will not serve the purpose.

Health information custodians may use personal health information for a variety of authorized purposes, including activities to improve or maintain the quality of care or the quality of any related programs or services of the custodian.

In limited circumstances, a health information custodian may disclose personal health information about an individual if the custodian believes on reasonable grounds that the disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons (i.e., a harm-reduction provision). In this and any type of disclosure to a non-

custodian, the recipient of the personal health information may use or disclose the information only for the original purpose for which the custodian was authorized to disclose the information under this Act or for the purposes of carrying out a legal duty.

The QCIPA permits the disclosure of information, including personal health information, to a quality of care committee created by a health facility in order to conduct a study, assessment, or evaluation towards the goal of improving or maintaining the quality of healthcare provided or the level of skill, knowledge, and competence of those who provide that healthcare. To do their work, quality of care committees may collect or prepare “quality of care information”, which is defined as information collected, submitted, or used for the sole or primary purpose of assisting such a committee in carrying out its functions, or information that relates solely or primarily to any activity that a quality of care committee conducts as part of its functions.

Quality of care information cannot be disclosed, except as permitted by the QCIPA. However, this category of information does not include information in a patient’s record that is maintained for the purpose of providing the patient with healthcare, nor does it include information that constitutes facts contained in a record of an incident involving the provision of healthcare to an individual, except if the facts involving the incident are also fully recorded in an individual’s record maintained for the purpose of providing healthcare to that individual. Accordingly, this kind of information is not caught by the disclosure limits that the Act places on quality of care information.

Furthermore, limits on the disclosure of quality of care information do not apply to disclosures to the management of the health facility that established the committee, nor do they apply if the

disclosure “is necessary for the purposes of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons” (which constitutes a harm-reduction provision).

Quebec

The review of Quebec legislation covered the *Charter of Human Rights and Freedoms*³¹ (also known as “the Charter”), the *Civil Code of Quebec*³² (also known as “the Civil Code”), *An Act Respecting Health Services and Social Services*^{33, 34}, the *Professional Code*,³⁵ *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*,³⁶ and *An Act Respecting the Protection of Personal Information in the Private Sector*.³⁷

Quebec’s *Charter of Human Rights and Freedoms* provides general protections for personal privacy and for nondisclosure of confidential information. It also provides for secrecy in judicial proceedings of information confided to a professional where that professional is bound by law to such secrecy.

The *Civil Code of Quebec* also provides general protections for privacy. Specifically, no one may invade the privacy of another person without the latter’s consent unless authorized to do so by law. In particular, information about an individual that is contained in a file created for a “serious and legitimate reason” may not be communicated to a third person and may not be used for an “inconsistent purpose” without the individual’s consent.

Within *An Act Respecting Health Services and Social Services* a “user’s” records are considered confidential, and no person may have access to them except with consent of the person or someone qualified to give consent on that person’s behalf.

In the case of a request for access to a user's record for the purpose of study, teaching, or research, consent must “free and enlightened” and must be given in writing. Other conditions

also apply. However, information contained in a record may be communicated without the person's consent under some circumstances. In one such circumstance, the director of professional services of an institution (or, if there is no such director, the executive director) may authorize a professional to examine the record of a user for study, teaching, or research purposes. Before granting such authorization, however, the director must ascertain that the criteria determined under section 125 of the *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* are satisfied. The authorization must be for a limited period, may be subject to conditions, and may be revoked at any time if confidentiality requirements are not met.

The equivalent of a harm-reduction provision allows an exception to the requirements for consent. This provision is narrow in scope, in that it applies to "information contained in the record of a user" that "may be communicated, in order to prevent an act of violence, including a suicide, where there is reasonable cause to believe that there is an imminent danger of death or serious bodily injury to the user, another person or an identifiable group of persons".

The organizational plan of an institution must also provide for the creation of a risk management committee. The functions of the committee include seeking, developing, and promoting ways to identify and analyze the risk of incidents or accidents, so as to ensure the safety of users and, particularly for nosocomial infections, to prevent such risks and reduce their recurrence. The committee must also establish a monitoring system, which would include creating a local register of incidents and accidents for the purpose of analyzing their causes and recommending to the institution's board of directors measures to prevent such incidents and accidents from recurring and any appropriate control measures.

Any information that flows during the course of risk management activities may not be used and may not be admitted as evidence against any person in a judicial or adjudicative proceeding. Furthermore, a risk manager or a member of a risk management committee may not be compelled to disclose such information. The records and minutes of a risk management committee are confidential and cannot be used, for example, to establish civil liability.

The *Act Respecting Health Services and Social Services* also creates requirements for reporting by employees and agents of the institution. As soon as possible after becoming aware of any incident or accident, an employee or agent must prepare a report for the executive director of the institution or his or her designate. The incident or accident is to be reported using a form provided for such purposes.

With a view to improving the health and well-being of the general public, the responsible minister must determine and implement priorities for health and social services. Though not yet in force—there is a provision in the act that directs the minister to establish (from the content of local registers) and maintain a register of “incidents” and “accidents” that have occurred during the provision of health services and social services. The purpose of the register is to monitor and analyze the causes of incidents and accidents, to ensure that measures are taken to prevent their recurrence, and to ensure that control measures are implemented, where appropriate.

A parallel provision exists within the *Professional Code*, which requires every professional to preserve the secrecy of all confidential information that becomes known to him or her, except with the authorization of the client or where ordered by law. However, a professional may communicate confidential information to prevent an act of violence, including a suicide, where there is reasonable cause to believe that there is imminent danger of death or serious bodily

injury to a person or an identifiable group of persons. However, only the information necessary to achieve these purposes may be communicated.

Under *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, the term “public bodies” includes health and social services institutions. Under this act, information concerning an individual that appears in any document and that allows the person to be identified is considered personal information. Such information is confidential, except where there is a valid consent to disclosure. In general, identifiable information—also termed “nominative information”— can be released with consent, or without consent in some cases; this includes release to a public body or an agency of another government if such release is necessary for the exercise of the rights and powers of the receiving body or the implementation of a program under its management. Release is also permitted to a person or a body where exceptional circumstances justify doing so. However, written agreement is required for release in this situation.

The Commission d'accès à l'information, established by section 103 of the *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* may, in response to a written request, authorize a person or an agency to receive, for study, research, or statistical purposes, personal information contained in a personal information file without the consent of the persons concerned, if the Commission feels that the intended use is not frivolous, that the ends contemplated cannot be achieved unless the information is communicated in a form allowing the persons to be identified, and that the personal information will be used in a manner that will ensure its confidentiality. Similar provisions exist for providing access for study, research, or statistical purposes to personal information about the professional activities of

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

professionals, provided that professional secrecy is maintained, the professionals are notified periodically of the intended uses and ends of the disclosure, the information is used only for the intended purpose, and the security of the information is maintained.³⁸

An Act Respecting the Protection of Personal Information in the Private Sector establishes particular rules with respect to the protection of personal information in accordance with articles 35 to 40 of the Civil Code, which refer to the handling of information while carrying on an enterprise within the meaning of article 1525 of the Civil Code, including a private medical clinic. For the purposes of this act, personal information is any information relating to an individual and allowing that person to be identified. Consent is required for release of such information to another party, unless the act provides for an exception. Where allowed by another Quebec statute or a collective agreement, such communication is permissible to a public body in keeping with its functions or a program, to a person or body having the power to compel communication of the information if required for the exercise of duties or functions to a person to whom the information must be communicated by reason of the urgency of a situation that threatens the life, health or safety of the person concerned; 8) to a person who is authorized to use the information for study, research or statistical purposes in accordance with section 21 or a person authorized pursuant to section 21.1, and to a person in accordance with section 22, in the case of a nominative list.

Nova Scotia

The following Nova Scotia legislation was reviewed: the *Freedom of Information and Protection of Privacy Act*³⁹ (FOIPPA) and the *Evidence Act*.⁴⁰

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

FOIPPA imposes requirements for the collection, use, and disclosure of personal information by public bodies, including hospitals. It also gives individuals access to their own personal information held by a public body. Although there are some limits on rights of access, patients do have the right to access their own medical or hospital records.

A third party may request disclosure of personal information by a public body, including a hospital. However, such disclosure would be deemed an unreasonable invasion of privacy if it were related to another individual's health information. Nevertheless, disclosure is not an unreasonable invasion of privacy if the individual has consented in writing to the disclosure or requested the disclosure. In determining whether a disclosure might be an unreasonable invasion of privacy, the head of the public body must consider all the relevant circumstances, including whether the disclosure is likely to promote public health and safety and whether the personal information was supplied in confidence.⁴¹ The disclosure is not an unreasonable invasion of privacy if there are compelling circumstances affecting someone's health or safety (another harm-reduction provision) or if some other act authorizes the disclosure.

Whether or not there is a request for access, a hospital may disclose information about a risk of significant harm to the health or safety of the public or a defined group of people or if the disclosures is otherwise clearly in the public interest. In this situation, the individual must be notified.

Nova Scotia's *Evidence Act* includes provisions that may place limits on information arising from hospital committees that have been established to study or evaluate care or practice. A witness in a legal proceeding is excused from answering any question about proceedings before this type of committee and is also excused from producing materials produced by such a

committee. However, this limitation does not apply to original medical and hospital records pertaining to a patient.

New Brunswick

The following statutes for New Brunswick were reviewed: the *Protection of Personal Information Act*⁴² (POPIA), the *Regional Health Authorities Act*⁴³ (RHAA), the *Hospital Act*⁴⁴, and the *Evidence Act*.⁴⁵

Through its Statutory Code of Practice, the New Brunswick POPIA governs public bodies, including regional health authorities and their hospitals, in their handling of personal information.⁴⁶ However, we had to identify other provincial statutes to better understand confidentiality provisions relevant to medication incident information.

The RHAA establishes 7 regional health authorities in 8 health regions within the province. Each regional health authority, overseen by a board of directors, is responsible for delivering and administering health services in its region. The board of directors must establish a professional advisory committee to provide advice about specific issues, including quality assurance and risk management. One regulation⁴⁷ of the RHAA permits the professional advisory committee to establish subcommittees and also allows the Minister to require a regional health authority to investigate any complaint about the care of a patient and to report its findings to the Minister.⁴⁸

Each regional health authority must compile a clinical record for each patient,^{49,50} including the person's identity and health information. Such clinical records must be kept confidential, except under specific circumstances, including a review of professional work in a community health centre operated by the regional health authority.

Although the RHAA generally prohibits disclosure of information relating to the health of an individual without that individual's consent, disclosures without consent are permitted in some circumstances, including if an advisory committee requires the information for quality assurance activities. Similarly, the *Hospital Act* and its regulations⁵¹ impose comparable requirements on regional health authorities to maintain records and keep them confidential. Again, some exceptions apply, including for disclosures related to a review of professional work in a hospital facility.

Certain provisions in the New Brunswick *Evidence Act* excuse a witness in a legal proceeding from providing or disclosing any information or producing any documents related to a proceeding before a committee that has been established by a regional health authority for the purpose of conducting any study, research, or program to improve medical or hospital care or practice. Similar restrictions apply to written or verbal opinions provided to such committees when they are investigating an occurrence, where such opinions relate to the standard of the medical or hospital care or practice that was provided by any person in the circumstances under investigation. However, these limits do not apply to records maintained by regional health authorities as required by the *Hospital Act*, the RHAA, and its regulations, nor do they apply to patient records.

Prince Edward Island

The following legislation from Prince Edward Island was reviewed: the *Freedom of Information and Protection of Privacy Act*,⁵²(FIPPA) the *Health Services Act*,⁵³ and the *Hospitals Act*.⁵⁴

The FIPPA places controls on the practices and procedures used by public bodies in handling personal information. Under this act, hospital standards committees and professional or technical

advisory committees are considered public bodies. The requirements and limits in the act apply to all records in the custody or under the control of a public body.

Personal information, including information relating to a person's health or healthcare, cannot be disclosed to an individual who applies for access to the information (an "applicant") if it would be an unreasonable invasion of a third party's personal privacy. Determining if a disclosure is "unreasonable" in this sense requires consideration of all relevant circumstances, including whether the disclosure is likely to promote public health and safety or environmental protection. However, disclosure of health information is permitted under some circumstances, including if the third party has given written consent or if there are compelling circumstances affecting anyone's health or safety and notice of the disclosure is mailed to the last known address of the third party (a harm-reduction provision).

Conversely, disclosure to an applicant may be refused, even if the information is *not* personal information about a third party. For example, if the information requested was generated from the activities of a committee of a public body, this would form a basis for refusal to disclose the information.

Whether or not access to information has been requested, the head of a public body must, without delay, disclose to the public, to an affected group of people, to any person, or to an applicant information related to a risk of significant harm to the environment or to the health or safety of the public, of the affected group of people, of the person, or of the applicant, or if such disclosure is clearly in the public interest. This requirement applies regardless of any other provisions of the FIPPA. Requirements for notice to the third party may apply. Disclosure is also permitted if the head of the public body believes, on reasonable grounds, that the disclosure will

avert or minimize an imminent danger to the health or safety of any person (a harm-reduction provision).

The *Health Services Act* sets out some limits similar to those in other evidence statutes in other provinces or territories, as already described. In particular, when a facility or hospital committee is conducting an internal investigation, it cannot compel an employee or committee member to produce documents or to disclose communications related to the investigations “in any matter” or in any action for negligence, malpractice, or breach.

The *Hospitals Act* permits disclosure of information relating to the health services provided to, or the medical condition of, any patient, without the patient’s consent, under certain limited conditions, including if the disclosure consists of non-identifying information that is disclosed for the purpose of improving the delivery of hospital services.

Newfoundland and Labrador

The following statutes from Newfoundland and Labrador were reviewed: the *Access to Information and Protection of Privacy Act* (ATIPPA),⁵⁵ the *Evidence Act*,⁵⁶ the *Hospitals Act*,⁵⁷ and the *Centre for Health Information Act*⁵⁸(CHIA).

The purposes of the ATIPPA are to make public bodies more accountable to the public and to protect personal privacy by various means, including prevention of the unauthorized collection, use, or disclosure of personal information by public bodies.

Hospital boards and authorities established under the *Hospitals Act* and health and community services boards established under the *Health and Community Services Act* are public bodies.

In general, the head of a public body must not disclose personal information, except if the individual making an application for access to the information is the individual to whom the

information relates or written consent to the disclosure has been provided. Disclosure without consent is permitted in some circumstances, including compelling circumstances affecting a person's health or safety and providing that notice of disclosure is mailed to the last known address of the third party to whom the information relates.

Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people, or to an applicant, information about a risk of significant harm to the environment or to the health or safety of the public or the group of people, when such disclosure is clearly in the public interest. This rule applies notwithstanding any other provision in ATIPPA. Notice requirements apply.

Part IV of the ATIPPA contains requirements for protection of privacy. Although these provisions had yet to be proclaimed at the time of this review,⁵⁹ they are relevant as models for best practice and so are included in this report. With regard to limits on the disclosure of personal information by public bodies, disclosure is permitted in certain specified circumstances, including where the head of the public body determines that there are compelling circumstances affecting a person's health or safety and where notice of disclosure is mailed to the last known address of the individual to whom the information relates, provided the disclosure is limited to the minimum amount of information necessary.

The *Evidence Act* applies to certain types of committees and various quality assurance and peer review committees, as defined under the *Hospital and Nursing Home Association Act* (now replaced by the *Health Care Association Act*⁶⁰). Accordingly, no report, statement, evaluation, recommendation, memorandum, document, or information of or made by, for, or to a committee can be disclosed in the course of a legal proceeding. A person who appears as a witness cannot

be asked and cannot answer any questions in connection with the proceedings of a committee, nor can such a witness produce a report, statement, evaluation, recommendation, memorandum, document, or information of or made by, for, or to a committee to which this section applies. However, these limits do not apply to original medical or hospital records pertaining to a specific person.

The *Hospitals Act* states that patient records are the property of the hospital authority. Access to hospital records is generally not permitted, nor is it permissible to disclose information contained in the records of the hospital authority, unless a specific exception applies, as is the case for disclosure to the patient involved. Anyone to whom personal information *is* disclosed cannot publish or further disclose the information if it could be detrimental to the personal interest, reputation, or privacy of a patient, a physician, a member of the staff of a hospital, or a person employed by the hospital authority. The *Hospitals Act* will be repealed and replaced by the *Regional Health Authorities Act*. The CHIA described below, will add the Newfoundland and Labrador Centre for Health Information to the list of entities to which personal information can be disclosed.

The CHIA was assented to on June 8, 2004, but at the time this report was drafted, it was not yet in force. Once proclaimed, the CHIA will establish the Newfoundland and Labrador Centre for Health Information as a corporation and crown agent. The CHIA will govern the centre in its activities, including activities involving the handling of personal information as defined in ATIPPA.

In operation since 1996, the centre facilitates decision-making that will enhance the health and well-being of provincial residents by providing a comprehensive, provincewide information

system. The centre is responsible for protecting the confidentiality and security of personal information that it collects, uses, discloses, stores, or disposes of and for providing accurate and current information to users of the health and community services system. Future regulations to the CHIA may create additional provisions regarding such items as administrative, technical, and physical safeguards for personal information at the centre, provisions of notice, and requirements for privacy impact assessments.

The CHIA contains a provision that will amend the *Health and Community Services Act* by adding a section to facilitate the release of information, including personal information as defined in the ATIPPA, to the centre by a board or the department.

The CHIA contains another provision that, once in force, will repeal subsection 35(3) of the *Hospitals Act*. The new provision will expand the specific exceptions to disclosure listed by permitting disclosure of information by a hospital authority to the Newfoundland and Labrador Centre for Health Information when the centre requests it in keeping with its objects and goals.

Yukon Territory

The following Yukon statutes were reviewed: the *Hospital Act*,⁶¹ the Hospital Standards (Yukon Hospital Corporation) Regulation,⁶² the *Access to Information and Protection of Privacy Act*⁶³ (ATIPPA), and the *Evidence Act*.⁶⁴

The ATIPPA ensures the accountability of public bodies and the protection of personal privacy. It gives individuals rights of access and correction regarding their own personal information and prevents unauthorized collection, use, or disclosure of personal information by public bodies in records that are under the control of a public body. However, as noted in the *Hospital Act*, the Yukon Hospital Corporation is not an agent of the government, and the privacy and access

provisions in the ATIPPA do not apply to the corporation. Instead, the corporation considers PIPEDA (the federal legislation) to apply to its handling of personal information.

The objectives of the Yukon Hospital Corporation include supplying hospital and medical care and services, as well as supervised residential care, continuing care, and rehabilitative care and services in the Yukon. Under the *Hospital Standards (Yukon Hospital Corporation) Regulation* to the *Hospital Act*, a hospital's board must make bylaws, including ones to establish committees to assess medical records, patient care, and other aspects of medical care and treatment within the hospital. The board must also establish and maintain a quality assurance program for the administration of clinical care within the hospital. The minister may also appoint one or more persons to investigate and report on the quality of the management and administration of a hospital and the quality of care and the treatment of patients in the hospital. An investigator may inspect and receive information about patient care from medical records or other sources and may reproduce or retain that information. The investigator may also interview hospital and medical staff about the care and services provided to a patient or to any class of patient in the hospital.

Under the *Evidence Act*, information about a proceeding before a hospital's quality assurance committee is not admissible in a legal proceeding. This provision covers documents or information about their content created by or for a committee where the purpose of the investigation, evaluation, or program was to facilitate medical education or to improve care or practice. However, these exclusions from legal proceedings do not apply to actual records maintained by a hospital as required by the *Hospital Act* or to medical or hospital records pertaining to a patient.

Northwest Territories and Nunavut

The following statutes from the Northwest Territories and Nunavut were reviewed: *Access to Information and Protection of Privacy Act* (ATIPPA),⁶⁵ the *Access to Information and Protection of Privacy Regulations* (ATIPPA Regulations),⁶⁶ the *Hospital Insurance and Health and Social Services Administration Act*,⁶⁷ the *Hospital and Health Care Facility Standards Regulations*,⁶⁸ and the *Evidence Act*.⁶⁹

The ATIPPA ensures the accountability of public bodies and the protection of personal privacy. It gives individuals rights of access and correction regarding their own personal information and prevents unauthorized collection, use, or disclosure by public bodies of personal information held in records or under the control of a public body. “Public bodies” include specific community health and social services boards. Schedule A of the ATIPPA Regulation specifies certain community health and social services boards that are public bodies under the act.

Individuals may make requests to access any record in the custody or under the control of a public body. However, the head of the public body must refuse such requests if the disclosure would be an unreasonable invasion of a third party’s personal privacy. This includes disclosures that relate to the health or healthcare of another individual. To determine if the disclosure is unreasonable in this way, the head must consider all of the relevant circumstances, including whether the disclosure is likely to promote public health and safety (a harm-reduction provision.) A head may also refuse disclosure where it could reasonably be expected to reveal such things as advice developed by or for a public body, the contents of agendas or minutes of meetings, or information that is subject to any type of privilege available at law, including solicitor–client privilege.

Disclosure is not considered an unreasonable invasion of privacy if there are compelling circumstances affecting the health or safety of any person and notice of the disclosure is mailed to the last known address of the third party. Disclosure for any purpose is also permitted when, in the opinion of the head of the public body, the public interest in disclosure clearly outweighs any invasion of privacy that could result.

Under the *Hospital and Health Care Facility Standards Regulations*, a hospital's health services committee must review and make recommendations to the chief executive officer with respect to any issue relating to a lack of improvement or to a complication in the condition of a patient or the death of a patient. The committee must also conduct periodic reviews of patients' medical files to study or evaluate healthcare practices and services for the purpose of determining methods for improvement. This review may only be conducted by committee members who are medical or professional staff or who are members retained under contract to perform services for the board of management.

According to the *Evidence Act*, a witness in legal proceeding cannot be asked and is not permitted to answer a question about a proceeding before a committee, nor can such a witness be asked or permitted to produce a document that was prepared by a committee exclusively for the purpose of improving medical care. Except in limited, specified circumstances, the committee must not disclose or publish a record of the committee or information submitted to or compiled for the committee. However, the restriction on documents does not apply to records maintained by hospitals or medical records pertaining to a patient.

Conclusions

As demonstrated in the preceding discussion, the sharing of medication incident information requires information that is both non-identifying and factual. While organizations must comply with the legislative rules in their own jurisdictions, general rules related to the privacy of personal information mean that medication incident information falls outside the application of statutory privacy rules. This is not necessarily the case for other types of incident data, but there is a strong argument to be made that statutory rules, in principle, support the sharing of information where the goal is to protect the safety of patients. The benefits of medication incident reporting and learning systems have been eloquently outlined in a World Health Organization report.⁷⁴ It is our considered opinion that, in all the jurisdictions in Canada, the general rules related to privacy of personal and personal health information and of quality-assurance-related opinions mean that *non-identifying facts* about an incident *are* sharable. We hope that the results of our study will aid health care practitioners and health service organizations in reassuring themselves about sharing of important information about preventable adverse drug events.

Recommendations

Reporting information about medication incidents

To determine whether the reporting of medication incidents (errors) is permissible under privacy and other applicable legislation, we had first to establish the type of information required for and contained in incident reports. For example, the following categories of information are received by the Institute for Safe Medication Practices Canada (ISMP Canada) from healthcare practitioners and institutions and will be used in this discussion as a model.⁷⁰

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

Specifically, ISMP Canada asks for the following information:

- a description of the incident or preventable adverse drug event
- the outcome of the adverse drug event
- the medication involved
- the type of incident
- the stage of the medication-use system involved
- the type of healthcare area or facility
- the type of healthcare professional discovering the incident

The following optional information may also be submitted:

- the age category and sex of the patient who was the subject of the incident
- a description of how the incident was discovered
- factors contributing to the incident
- any recommendations of the practitioner or institution to prevent similar incidents in the future
- contact information for the person making the report to ISMP Canada

The following types of information are excluded from these reporting categories:

- the name and contact information of the patient who was the subject of the incident
- unique identifying numbers (such as provincial health card number or a local hospital file number) used in providing treatment
- information about the professional or treatment relationship between the person reporting the incident and the patient who was the subject of the incident

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

Definitions in statute—identifiability of information

As discovered in the review of legislation summarized in the previous section, each Canadian province and territory has at least one statute (consisting of both legislation and accompanying regulations, but often referred to interchangeably with the term “legislation”) that governs the collection, use, and disclosure of personal information, either including or specific to personal health information. The statutes do not apply to all types of organization or person, but rather to specific types of entities. Consider the following examples:

- Most legislation titled “Freedom of Information and Protection of Privacy Act” (often indicated by the acronym FIPPA or FOIPPA) and “Access to Information and Protection of Privacy Act” (often indicated by the acronym ATIPPA) or a similar title, represents public sector statutes, with application to “public bodies”, often including public hospitals.
- In Ontario, hospitals are not considered “public bodies” under the province’s FIPPA; however, they are included in the definition of “health information custodian” in the *Personal Health Information Protection Act, 2004* (PHIPA), as are regulated health professionals.
- In British Columbia, where there is no statute specific to health information, there is both public sector legislation (the FIPPA), which regulates public bodies, including hospitals, and private sector legislation (the PIPA), which regulates various private entities, including private physicians’ offices.
- In contrast, the Yukon Hospital Corporation is incorporated under statute but is specifically exempted from the category of “public body” congruent to the meaning

within the territory's ATIPPA. Some limits on the disclosure of information in patient records are set out in the Yukon regulations. Nevertheless, in the absence of territory-specific protections for personal health information, the federal privacy statute (*Personal Information Protection and Electronic Documents Act*) would apply. While not specific to health information privacy, the 10 fair information practices that are the foundation of that statute set a common standard across Canada.

Despite the variations in the application of privacy statutes and privacy rules, all statutes contain definitions of the type of information to which the statute applies and the type of information that constitutes “personal information” (or a similar phrase.) Common among all the definitions of “personal information” is the requirement for a threshold degree of identifiability: in order for the information to fall within the definition, it must be *about* an identifiable individual.

Incident data—identifiable or not?

The importance of establishing whether incident data are or are not identifiable is that non-identifiable information falling outside the definitions of “personal information” will also fall outside the application of the statute. In other words, statutory rules that impose limits on disclosure of patients’ personal information apply to identifiable information. Where the information is not identifiable—i.e., is not “personal information” as defined in the statute—the statute does not apply. In determining whether information is identifiable, the reporter must also consider the potential for shared information to be linked with other sources of information. If we follow the description of medication incident data above as an example, incident data need not be identifying data.

Re-identification of data—possibility versus foreseeability

Under some circumstances, it may be possible for incident information that is not identifiable to be correctly associated with information from other sources, thereby becoming “re-identified” and capable of being used to identify an individual. When considering the potential for re-identifying previously non-identifiable information, it is important to distinguish between the possibility of identifying an individual and the foreseeability of doing so. As a general rule, the law does not require standards of perfection: due diligence in following statutory privacy rules does not require anticipation of each and every possibility for re-identification. Rather, it requires turning one’s mind to foreseeable circumstances that are likely to arise (rather than highly remote circumstances) to determine if re-identification might occur. A requirement to anticipate all (or even most) possible circumstances in which re-identification might occur would render the task of developing policies for data-sharing impossible.

Statute-protected information

Whether or not incident information is identifiable—and therefore whether or not it is “personal information” according to privacy statutes—additional limits on sharing incident information may apply. The sources of these limits are often found in statutes other than privacy legislation. As described in section III, some jurisdictions have general prohibitions on disclosure, such that incident-related information flowing to a quality of care committee cannot subsequently be disclosed. Such information also cannot be used in a legal proceeding. These limits protect incident review information that is collected by or submitted to a specially designated committee with powers granted by statute to investigate or review one or more events that have adversely affected patient care. However, what constitutes “protected information” is narrow in scope; it

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

includes information submitted to or requested by such a committee specifically for its purposes but does not include information that originates in a patient’s treatment record or that is sourced from another record of an incident. In other words, factual information about the care and condition of a patient who was the subject of an incident that originates in other records (e.g., patient treatment files) is not “protected information”.

In general, the impetus for casting a kind of evidentiary privilege on protected information is to create a context in which health professionals can communicate frankly with this type of committee their opinions about the adverse event, without concerns for reprisal or liability. The hope is that such frankness will enable the committee to investigate thoroughly and make recommendations that will improve education and policy and ultimately prevent or at least mitigate similar events in the future. For this reason, once information is collected by or submitted to this type of statutorily authorized committee for its purposes and designated as review information, there are very strict and understandable limits on disclosure.

Medication incident data—non-identifiable and factual information is also disclosable information

Insofar as the sources of factual information are patients’ medical records, statutory privacy rules apply to the disclosure of identifiable information. However, where that information is not identifiable according to the relevant definition, the information falls outside privacy statutory rules and the limits on disclosure of identifiable personal information do not apply. Furthermore, insofar as information submitted to a committee is derived from facts originating in a patient file, it will not be caught by rules of privilege. In other words, it is possible to disclose information that is both non-identifiable and factual.

Let us return to the list at the beginning of section IV, which describes the types of information that ISMP Canada requests from reporters. If we are correct in contending that:

- 1) insofar as the information supplied is about the incident that occurred and is not about the person who was the subject of the incident and
- 2) insofar as the information is factual in nature and could be retrieved from sources that exist independent of any type of protected enquiry or quality assurance committee,

then medication incident data assembled according to the categories in the list can be shared, at least for valid purposes (e.g., education and risk management) and certainly for purposes and processes to avert future risks of harm.

Nevertheless, we believe that the scope of the statutory limits discussed above have occasionally been misinterpreted as overly broad. As a result, the limits on the sharing of incident data—particularly, in our experience, medication incident data—have sometimes been misunderstood (and are seen as being just as restrictive as limits on identifiable personal health information.)

This type of misunderstanding may be, at least in part, the basis for the types of concerns expressed in *Building a Safer System* and the recommendation of the National Steering Committee on Patient Safety that privacy legislation be standardized. Given that effective incident data are (or can be) factual, and given that such data meet all tests for being non-identifiable, what is really needed is a set of nationally accepted categories of data elements to be used for reporting medication incidents (and indeed all types of incidents) across Canada. Where these categories would be used consistently by all persons and organizations collecting and using incident data, and where all such data were foreseeably both non-identifying and factual, the

collection of data according to a single “standard” would overcome privacy and other confidentiality concerns.

Potential models for harmonized incident reporting—inspiration from the Saskatchewan Critical Incident Reporting Guideline

As discussed earlier, the statutes in Saskatchewan create a system of rules that mandate the reporting of “critical incidents”, as defined in statute. The guideline lists 6 categories of events that must be reported to Saskatchewan Health by regional health authorities and healthcare organizations: (I) surgical events (including endoscopy and other invasive procedures), (II) product or device events, (III) patient protection events, (IV) care management events, (V) environmental events, and (VI) criminal events. The regulations limit the collection of identifying information insofar as names are not included (i.e., the name of any person to whom the critical incident relates, the name of any healthcare provider involved in providing health services to any person described or any person involved in operating a program to which the critical incident relates, or the name of any other individual who has knowledge of the critical incident.)

In addition to their place in the Saskatchewan statutory scheme, these categories might serve as a template or model for conceptualizing and organizing incident information into functional categories for other systems of incident reporting. Each category is further broken down into lists of event types or subcategories. For example, the category of care management events includes medication incidents, which are care management events occurring when “(a) patient death or serious disability associated with a medication or fluid error including, but not limited to, errors involving the wrong drug, the wrong dose, the wrong patient, the wrong time, the wrong rate, the

This project is partially funded by:



Striking a Balance: Facilitating Access to Patient Safety Data While Protecting Privacy Through Creation of a National Harmonized Standard

Investigators:
Weisbaum et al., 2007

wrong preparation, or the wrong route of administration. (Excludes reasonable differences in clinical judgment on drug selection and dose.)” As noted earlier, the definition of “medication incident” includes “any preventable event that may cause or lead to inappropriate medication use or patient harm while the medication is in the control of the health-care professional, patient, or consumer. Medication incidents may be related to professional practice, drug products, procedures, and systems, and include prescribing, order communication, product labelling/packaging/nomenclature, compounding, dispensing, distribution, administration, education, monitoring, and use.”⁷¹ This description is not the same as, but is consistent with, the description of care management events in the Saskatchewan guidelines.

The Saskatchewan guidelines set out what is clearly a mandatory scheme for reporting critical incidents. This type of legislated scheme typically works to authorize the collection of information without consent for the sake of the benefits that will flow from the collection and use of such information. But if this scheme is to be used as a model or template for other non-mandatory reporting systems, the information must be de-identified so that it falls outside definitions of “personal information” to which the various legislative acts apply (unless the information is to be collected with consent or under a specified exception). The fact that names are not collected is not sufficient to ensure that information is de-identified to the extent that it falls outside definitions of “personal information” and similar terms. As a general rule, the removal of names contributes to confidentiality of information but does not necessarily ensure de-identification. This point may be even clearer if consideration is given to Saskatchewan’s legislation regarding the privacy of health information, HIPA. Under that legislation, de-identified personal health information is “personal health information from which any

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

information that may reasonably be expected to identify an individual has been removed”. Even if names are removed, other information left behind may or may not meet this test for “de-identification”. To ensure an adequate degree of de-identification, other parameters will need to be added. In other words, a more precise description would be required of the data that would be collected under something like category IV(a) of the Saskatchewan guidelines.

This requirement could be met (at least in the case of medication incident information) if the data elements described earlier (i.e., the ones collected by ISMP Canada for the purpose of medication incident analysis) were specified under category IV(a) in order to establish the scope of the information collected. Recall that these data elements relate to the incident that occurred, not the person who was the subject of the incident; and that the information is factual in nature and could be retrieved from sources that exist independent of any protected enquiry or quality assurance committee.

Where medication incident data are limited to data that fall within this list, the information shared would be brought significantly closer to meeting any test of “de-identification” (using Saskatchewan’s HIPA as an example) insofar as the data elements do not include information that “may reasonably be expected to identify an individual.” To ensure that the information collected is de-identified, a specific data set would need to be established. Also, and as a matter of best practice, individuals involved in handling such information would receive privacy training to ensure that they were sensitized to any unforeseen issues that might arise during sharing processes. If a national consensus could be reached on the minimal content of the data set, and if standardized training were developed, there is great potential that information-sharing would be compliant with statutes. This is not to imply that information should be shared with no

regard to purpose or limits—a combination of ethics and policy can be implemented to require that information be shared only for valid purposes. A national approach can ensure that information-sharing is respectful of privacy while upholding the values of transparency for the sake of the public good.

If similar lists for other categories and subcategories of incidents could be developed, and if tests and other requirements for de-identification could be met, then compliance with statutory rules and values of transparency might be possible for the purpose of facilitating the sharing of information about other types of incidents.

Harm-reduction provisions and their significance for incident reporting

It is not uncommon to think of statutes and corresponding procedural factors as limiting information flows. It is also easy to forget that statutes often enable flows, serving as a source of authorization for mandated and valid activities. In the absence of express or clear authorization, it may be useful to review and consider the legislative and policy intent behind a statute. Clearly, the main goals of privacy statutes are to protect individuals' personal privacy and to uphold requirements for confidentiality. Yet the protection of privacy was never intended to trump any and all other claims. Rather, the requirement for privacy must be balanced against public welfare and safety, and appeals to privacy entitlements should not necessarily override serious concerns about potential harm. The idea that the safety of individuals and the public should be paramount in these situations is exemplified in these provisions, and appealing to the policy intent behind these provisions may be a useful strategy to facilitate information flows.

With this in mind, we examined some statutory provisions that permit the disclosure of personal information or personal health information under certain particular circumstances. Typically, the

kinds of provisions that we reviewed occur in privacy legislation and supply an exception (sometimes a very narrow exception) to general rules about disclosure. To describe these provisions very generally, they permit the sharing of personal information (without consent or the need for a more specific exception) where doing so will facilitate avoidance of a risk of harm. Some of these provisions are limited to very specific circumstances.

Our review of legislation conducted for this project and our related discussions prompted us to think more about these particular types of provisions. This is partly because, unlike some other kinds of incident reporting, medication incidents may be characterized by an urgent or pressing need for relevant information in order to prevent further occurrences of the incident. Because a detailed discussion of harm-reduction provisions falls outside of the original goals of this paper, we have decided to simply mention at this time that these provisions exist and require further exploration. It is not our intention to argue for or against the claim that harm-reduction provisions apply to incident information that may be identifiable (as we have already established, medication incident data need not be identifying information). Rather, we think that these provisions are examples of existing statutory “clues” to the justification of the need for balancing privacy of identifying information with justifiable needs for information to be shared, including in order to notify healthcare providers and hospitals about the fact that an incident has occurred where that type of error is reasonably likely to occur again. Insofar as such provisions might be applicable in this context, we have noted such provisions in the table at the end of this section.

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

Ethics and the benefits of transparency

Where rules regarding the identifiability of information and privilege do not apply, it may be difficult from an ethics perspective to justify placing limits on the sharing of incident data, in particular where the benefits of sharing have already been demonstrated.

Consider the example of a US database, the Manufacturer and User Facility Device Experience Database⁷²(MAUDE.) While this database is not a made-in-Canada example, it is described below in order to demonstrate that events can be shared openly as a way to facilitate learning. It sets a precedent for transparency. MAUDE data represents reports of adverse events involving medical devices. The database includes voluntary reports since June 1993, user facility reports since 1991, distributor reports since 1993, and manufacturer reports since August 1996. MAUDE may not include reports made according to exemptions, variances, or alternative reporting requirements granted under Title 21 of the Code of Federal Regulations, which is reserved for rules of the Food and Drug Administration (FDA).⁷³

MAUDE permits online searches of the Center for Devices and Radiological Health database, including information on medical devices that may have malfunctioned or caused a death or serious injury. Searches retrieve records that contain the search term(s) provided by the user, including the ability to search by medication involved. The FDA aims to include all reports received before quarterly updates.

MAUDE data are not intended to be used either to evaluate rates of adverse events or to compare adverse event occurrence rates across devices. However, the potential benefits of a database like MAUDE lies in its transparency; this database clearly provides proof of the ability to share relevant learning about preventable adverse events. Ideally, a worldwide standard taxonomy and

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007

database (e.g., facilitated through an organization such as the World Health Organization) would permit the various local and national external reporting programs to contribute to an international aggregate database.

Categories of Information to be considered for rules about sharing related to incident reporting

In sorting through the statutory rules and the framework for this report, we devised a draft system for organizing or categorizing the rules that apply to the sharing of medication incident data. It is set out in the table below. Although these categories probably do not cover all possible types of sharing, they seem to fit with what we found in the statutes, and the scheme may provide a basis for developing approaches to the sharing of other types of incident data.

Category	Rule for disclosure or sharing for the purpose of incident reporting
1. Information that is not identifiable (i.e., not defined under a statute as personal information [PI] or personal health information [PHI]) and is not protected information (i.e., is factual information)	This category of information can be disclosed/shared for the purpose of incident reporting.
2. Information that is identifiable (i.e., is PI or PHI) and for which the patient and/or a surrogate has provided consent to disclose	This category of information can be disclosed/shared for the purpose of incident reporting.
3. Information that is identifiable (i.e., is PI or PHI), but the exceptional circumstances of the incident meet a test of a harm-reduction provision that is set out in a key statute	This category of information can be disclosed/shared for the purpose of incident reporting.
4. Information that is not identifiable (i.e., is not PI or PHI), but is protected information	This category of information cannot be disclosed/shared for the purpose of incident reporting.
5. Information that is not identifiable (i.e., is not PI or PHI), but is protected information and there are exceptional circumstances that meet a test of a harm-reduction provision set out in a key statute	This category of information can be disclosed/shared for the purpose of incident reporting.
6. Information that is identifiable (i.e., is PI or PHI), is protected information, or both, but to which an exception applies (i.e., in the scope of this report, it would be a statutory exception, for example, where reporting is required by law or permitted by a special statute)	This category of information can be disclosed/shared for the purpose of incident reporting.
7. Information that is identifiable (i.e., is PI or PHI) and there is no exception, no consent, and no circumstances that meet a harm-reduction provision	This category of information cannot be disclosed/shared for the purpose of incident reporting.

This project is partially funded by:



Striking a Balance: Facilitating Access to Patient Safety Data While Protecting Privacy Through Creation of a National Harmonized Standard

Investigators:
Weisbaum et al., 2007

References

- 1) This research project was funded in part through research funding from the Canadian Patient Safety Institute (CPSI) and through in-kind contributions from the home institutions of each coauthor: Queen's University and Biotika Inc., Montréal (K. Weisbaum), Institute for Safe Medication Practices Canada (S. Hyland), and the Healthcare Insurance Reciprocal of Canada (HIROC) (E. Morton.)
- 2) National Steering Committee on Patient Safety. Building a safer system: a national integrated strategy for improving patient safety in Canadian health care. Ottawa (ON): Royal College of Physicians and Surgeons of Canada; 2002 [cited February 2007]. Available from: http://rcpsc.medical.org/publications/building_a_safer_system_e.pdf
- 3) Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. Available from: <http://www.canlii.org/ca/sta/p-8.6>; Schedule 1, Principles set out in the national standard of Canada entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96. Available from: <http://www.canlii.org/ca/sta/p-8.6/part288829.html>; [cited 2007 Jul 7].
- 4) Collins PC, Slaughter PM, Roos N, Weisbaum KM, Hirtle MH, Williams JI, Martens P., Laupacis A, Harmonizing research and privacy: standards for a collaborative future. Toronto (ON): Institute for Clinical Evaluative Sciences; 2006 [cited February 2007]. Available from: http://www.ices.on.ca/WebBuild/site/ices-internetupload/file_collection/Harmonizing%5FResearch%5FPrivacy%5FFinal%20Report%20Epdf
- 5) A medication incident reporting and prevention system for Canada: business plan. Ottawa (ON): Canadian Coalition on Medication Incident Reporting and Prevention; 2002 [cited March 2008] Available from: http://www.hc-sc.gc.ca/dhp-mps/medeff/research-recherche/cmirms-scdpim_reprapp_e.html
- 6) Definition of terms. Toronto (ON): Institute for Safe Medication Practices Canada; [cited 2007 Mar 27]. Available from: <http://www.ismp-canada.org/definitions.htm>
- 7) Baker GR, Norton PG, Flintoft V, Blais R, Brown A, Cox J, et al. The Canadian Adverse Events Study: the incidence of adverse events among hospital patients in Canada. CMAJ. 2004;170(11):1678-1686.
- 8) Kohn LT, Corrigan JM, Donaldson MS, editors; Institute of Medicine, Committee on Quality of Health Care in America. *To err is human: building a safer health system*. Washington (DC): National Academy Press; 1999.
- 9) Baker RG, Norton P. Patient Safety and Healthcare Error in the Canadian Healthcare System. A Systematic Review and Analysis of Leading Practices in Canada with Reference

This project is partially funded by:



Striking a Balance: Facilitating Access to Patient Safety Data While Protecting Privacy Through Creation of a National Harmonized Standard

Investigators:
Weisbaum et al., 2007

to Key Initiatives Elsewhere. A Report to Health Canada. [Cited March 2008] Available from: http://www.hcsc.gc.ca/hcs-sss/pubs/qual/2001-patient-securit-rev-exam/index_e.html

- 10) Suydam S, Liang BA, Anderson S, Weinger MG. Patient safety data sharing and protection from legal discovery. In: Clancy C, Tornberg DN, editors. *Advances in patient safety: from research to implementation*. Vol 3: Implementation issues. p. 361-370. AHRQ Publ No. 050021-3. Rockville (MD): Agency for Healthcare Research and Quality; 2005. Available from: <http://www.ahrq.gov/downloads/pub/advances/vol3/Suydam.pdf>
- 11) Liang BA. Weinger MB. Suydam S. Learning from others: legal aspects of sharing patient safety data using provider consortia. *J Patient Saf*. 2005;1(2):83-89.
- 12) Phillips RL, Dovey SM, Hickner JS, Graham D, Johnson M. The AAFP Patient Safety Reporting System: development and legal issues pertinent to medical error tracking and analysis. In: Clancy C, Tornberg DN, editors. *Advances in patient safety: from research to implementation*. Vol 3: Implementation issues. p. 121-134. AHRQ Publ No. 05-0021-3. Rockville (MD): Agency for Healthcare Research and Quality; 2005. Available from: <http://www.ahrq.gov/downloads/pub/advances/vol3/Phillips.pdf>
- 13) Gilmour GM. Patient safety, medical error, and tort law: an international comparison. Ottawa (ON): Health Canada; 2006. Available from: http://www.hc-sc.gc.ca/sr-sr/finance/hprpprps/results-resultats/2006-gilmour_e.html
- 14) Note this comment from the Hansard debates: “Protections of some types of information in the *Evidence Act* are designed to ensure the confidentiality of information provided to committees that evaluate medical staff and medical programs for the purpose of improving health care. These apply to a very limited range of records and do not apply to a patient's own personal records or to any documents gathered in the course of treatment or care.” British Columbia. Legislative Assembly. Official Report of Debates of the Legislative Assembly (Hansard). 35th Parliament, 4th Session. Vol 20, no. 19 (1995 Jun 6) [cited 2006 May 31]. p. 15001.
Available from: <http://www.leg.bc.ca/hansard/35th4th/h0606am.htm#15001>.
- 15) Personal Information Protection Act SBC 2003 c. 63. Available from: http://www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm; [cited 2007 Jul 7].
- 16) “Personal information” is defined in PIPA as recorded information about an identifiable individual, but it does not encompass contact information at an individual’s place of business. This term has been interpreted by the Office of the Information and Privacy Commissioner of British Columbia, the British Columbia Medical Association, and the Collage of Physicians and Surgeons of British Columbia as including an individual’s personal health information, sex, age, ethnic origin, race, and identification numbers.

Incident data that are not identifiable (i.e., are not “about an identifiable individual”) would fall outside the definition of “personal information” and would not be caught by PIPA.

- 17) The implication of this statement is that information flowing from patient records would not be limited by s. 51. Furthermore, if the information flowing from the record is not identifiable according to definitions in either FIPPA or PIPA, it would not be excluded from incident reporting, at least not if it is not part of a “record” submitted to a committee, as described in subsection 51(2).
- 18) Health Information Act, R.S.A. 2000, c. H-5. Available from: <http://www.canlii.org/ab/laws/sta/h-5/20080215/whole.html>; [cited 2008 Mar 3].
- 19) Alberta Evidence Act, R.S.A. 2000, c. A-18. Enabled Regulation: Quality Assurance Committee Regulation, Alta. Reg. 294/2003. Available from: <http://www.canlii.org/ab/laws/sta/a-18/20080215/whole.html>; [cited 2008 Mar 3]
- 20) Regional Health Services Act, S.S. 2002, c. R-8.2. Available from: <http://www.canlii.org/sk/laws/sta/r-8.2/20080215/whole.html>; [cited 2008 Mar 3]
- 21) Critical Incident Regulations, R.R.S. c. R-8.2 Reg. 3. Available from: <http://www.canlii.org/sk/laws/regu/r-8.2r.3/index.html>; [cited 2007 Jul 7].
- 22) Health Information Protection Act, S.S. 1999, c. H-0.021 (Enabled Regulation: Health Information Protection Regulations, R.R.S. c. H-0.021 Reg. 1). Available from: <http://www.canlii.org/sk/laws/sta/h-0.021/20080215/whole.html>; [cited 2008 Jul 7].
- 23) Evidence Act, S.S. 2006, c. E-11.2. Available from: <http://www.canlii.org/sk/laws/sta/e-11.2/20080215/whole.html>; [cited 2007 Jul 7].
- 24) Reports must include a description of the circumstances leading up to and culminating in the critical incident; a statement identifying any current practice, procedure, or factor involved in the provision of the health service or the operation of the program that contributed to the occurrence of the critical incident and that might, if corrected or modified, prevent the occurrence of a similar critical incident in the future; and a description of the actions taken and the actions intended to be taken by the regional health authority as a result of the investigation and any recommendations arising from the investigation.
- 25) Personal Health Information Act, C.C.S.M. c. P33.5. Enabled Regulation: Personal Health Information Regulation, Man. Reg. 245/97. Available from: <http://www.canlii.org/mb/laws/sta/p-33.5/20080215/whole.html>; [cited 2007 Jul 7]
- 26) Regional Health Authorities Act, C.C.S.M. c. R34. Available from: <http://www.canlii.org/mb/laws/sta/r-34/20080215/whole.html>; [cited 2008 Mar 3].

- 27) The Regional Health Authorities Amendment and Manitoba Evidence Amendment Act S.M. 2005, c. 24. Available from: <http://web2.gov.mb.ca/laws/statutes/2005/c02405e.php>; [cited 2006 Oct 3].
- 28) There is no elaboration in PHIA about the specific characteristics of meaningful consent involved in obtaining and managing personal information. However, the office of the Ombudsman of Manitoba provides information and practical guidance on generic elements of informed consent. See <http://www.ombudsman.mb.ca/pdf/PHIA%20--%20A4%20Elements%20of%20Consent%202004-06-09.pdf>
- 29) Personal Health Information Protection Act, S.O. 2004, c. 3, Schedule A. Amended 2005, c. 25, s. 35; 2006, c. 4, s. 51; 2006, c. 17, s. 253. Available from: http://www.elaws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm; [cited 2008 Mar 3].
- 30) Quality of Care Information Protection Act, 2004, S.O. 2004, c. 3, Sch. B. Available from: <http://www.canlii.org/on/laws/sta/2004c.3sch.b/20080215/whole.html>; [cited 2007 Jul 7].
- 31) Charter of Human Rights and Freedoms, R.S.Q., c. C-12. Available from: <http://www.ijcan.org/qc/laws/sta/c-12/index.html> [cited 2008 Mar 3].
- 32) Civil Code of Quebec, L.Q. 1991, c. 64. Available from: <http://www.ijcan.org/qc/laws/sta/ccq/index.html> [cited 2008 Mar 3].
- 33) An Act Respecting Health Services and Social Services, R.S.Q., c. S-4.2 Available from: <http://www.ijcan.org/qc/laws/sta/s-4.2/index.html> [cited 2008 Mar 3].
- 34) *The HSSS act* distinguishes between “accident” and “incident”: “‘Accident’ means an action or situation where a risk event occurs which has or could have consequences for the state of health or welfare of the user, a personnel member, a professional involved or a third person” [section 8]. “‘Incident’ means an action or situation that does not have consequences for the state of health or welfare of a user, a personnel member, a professional involved or a third person, but the outcome of which is unusual and could have had consequences under different circumstances” [section 183.2].
- 35) Professional Code, R.S.Q., c. C-26. Available from: <http://www.ijcan.org/qc/laws/sta/c-26/index.html> [cited 2008 Mar 2].
- 36) An Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information, R.S.Q., c. A-2.1. Available from: <http://www.ijcan.org/qc/laws/sta/a-2.1/index.html> [cited 2008 Mar 3]

- 37) An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., c. P-39.1. Available from: <http://www.ijcan.org/qc/laws/sta/p-39.1/index.html> [cited 2008 Mar 3].
- 38) There were divergent opinions between the Commission d'accès à l'information (Québec) and the Privacy Commissioner of Canada on the activities of IMS Canada.
- 39) Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5. Available from: <http://www.canlii.org/ns/laws/sta/1993c.5/20060718/whole.html> [last update 2006 Jul 18; cited 2006 Jul 18]. Enabled regulation: Freedom of Information and Protection of Privacy Regulation, N.S. Reg. 105/94. Amended 1999 (2nd Sess.), c. 11; 2002, c. 5, ss. 18, 19; 2004, c. 4, s. 112).
- 40) Evidence Act, R.S.N.S. 1989, c. 154; amended 1995-96, c. 13, s. 79; 1999 (2nd Sess.), c. 8, s. 5; 2001, c. 6, s. 105; 2002, c. 17 Available from: <http://www.canlii.org/ns/laws/sta/r1989c.154/20060718/whole.html> [cited 2008 Mar 3].]
- 41) Like most other privacy legislation, the Freedom of Information and Protection of Privacy Act here is based on an authorization model, rather than a consent model, so consent is not required for collection of personal information by a public body, such as a hospital. However, collection of information must be for a legitimate purpose, which includes the operation of a program or activity.
- 42) Protection of Personal Information Act, S.N.B. 1998, c. P-19.1. Available from: <http://www.canlii.org/nb/laws/sta/p-19.1/20060927/whole.html>; [cited 2006 Oct 17].
- 43) Regional Health Authorities Act, S.N.B. 2002, c. R-5.05. Available from: <http://www.canlii.org/nb/laws/sta/r-5.05/20060927/whole.html>; [cited 2006 Oct 17].
- 44) Hospital Act, S.N.B. 1992, c. H-6.1; Available from: <http://www.canlii.org/nb/laws/sta/h-6.1/20060927/whole.html>; [cited 2006 Oct 17].
- 45) Evidence Act, R.S.N.B. 1973, c. E-11 Available from: <http://www.canlii.org/nb/laws/sta/e-11/20060718/whole.html>; [cited 2006 Oct 13].
- 46) "Personal information" means information about an identifiable individual, recorded in any form. This expressly excludes information collected, used, or disclosed in a form in which the individual is not identifiable. An individual is identifiable if the information includes his or her name, makes his or her identity obvious, or is likely in the circumstances to be combined with other information that does.
- 47) General Regulation – Regional Health Authorities Act, N.B. Reg. 2002-27; Available from: <http://www.canlii.org/nb/laws/regu/2002r.27/20060927/whole.html> [cited 2006 Oct 17].

- 48) Enabling statute: Regional Health Authorities Act, S.N.B. 2002, c. R-5.05; consolidation: 2004 May 7.
- 49) While it is not explicit in the RHAA or its regulations, it is conceivable that such an investigation could be conducted by a committee or a subcommittee.
- 50) Community Health Centres Regulation – Regional Health Authorities Act, N.B. Reg. 2002-87; Available from: <http://www.canlii.org/nb/laws/regu/2002r.87/20060718/whole.html> [cited 2002 Dec 31]. Enabling statute: Regional Health Authorities Act, S.N.B. 2002, c. R-5.05; consolidation: 2002 Dec 31.
- 51) A similar requirement is included in the General Regulation – Regional Health Authorities Act, N.B. Reg. 2002-27 Available from: <http://www.canlii.org/nb/laws/regu/2002r.27/20060927/whole.html>; [cited 2006 Oct 17].
- 52) General Regulation – Hospital Act, N.B. Reg. 92-84; Available from: <http://www.canlii.org/nb/laws/regu/1992r.84/20060927/whole.html>; [cited 2006 Oct 17].
- 53) Freedom of Information and Protection of Privacy Act, R.S.P.E.I. 1988, c. F-15.01. Available from: <http://www.canlii.org/pe/laws/sta/f-15.01/20060926/whole.html>; [cited 2006 Oct 19].
- 54) Health Services Act, R.S.P.E.I. 1988, c. H-1.5. Available from: <http://www.canlii.org/pe/laws/sta/h-1.5/20060926/whole.html> [cited 2006 Oct 20].
- 55) Hospitals Act, R.S.P.E.I. 1988, c. H-10.1. Available from: <http://www.canlii.org/pe/laws/sta/h-10.1/20060926/whole.html> [cited 2007 Jul 7].
- 56) Access to Information and Protection of Privacy Act, S.N.L. 2002, c. A-1.1. Available from: <http://www.canlii.org/nl/laws/sta/a-1.1/20060809/whole.html> [cited 2006 Nov 3].
- 57) Evidence Act, R.S.N.L. 1990, c. E-16. Available from: <http://www.canlii.org/nl/laws/sta/e-16/20060809/whole.html> [cited 2006 Oct 13].
- 58) Hospitals Act, R.S.N.L. 1990, c. H-9. Available from: <http://www.canlii.org/nl/laws/sta/h-9/20060809/whole.html> [cited 2006 Nov 5].
- 59) Centre for Health Information Act, S.N.L. 2004, c. C-5.1. Assented to 2004 Jun 8, not yet proclaimed. Available from: <http://www.canlii.org/nl/laws/sta/c-5.1/20060809/whole.html> [cited 2006 Nov 5].

- 60) At a future time, the Lieutenant-Governor in Council may make regulations defining "personal health information" for the purpose of a proclamation of the privacy provisions of ATIPPA [s. 73(r), s. 77 generally]; however, such provisions do not currently exist.
- 61) Health Care Association Act, R.S.N.L. 1990, c. H-8, section 3. Available from: <http://www.canlii.org/nl/laws/sta/h-8/20060809/whole.html>; [cited 2006 Nov 2].
- 62) Hospital Act, R.S.Y. 2002, c. 111. Available from: <http://www.canlii.org/yk/laws/sta/111/20060728/whole.html>; [cited 2006 Nov 5].
- 63) Hospital Standards (Yukon Hospital Corporation) Regulation, Y.O.I.C. 1994/227. Available from: <http://www.canlii.org/yk/laws/regu/1994r.227/20060728/whole.html> [cited 2006 Nov 5]. Enabling statute: Hospital Act, R.S.Y. 2002, c. 111.
- 64) Access to Information and Protection of Privacy Act, R.S.Y. 2002, c. 1. Available from: <http://www.canlii.org/yk/laws/sta/1/20060728/whole.html> [cited 2006 Nov 5]. Enabled regulation: Access to Information Regulation, Y.O.I.C. 1996/053.
- 65) Evidence Act, R.S.Y. 2002, c. 78. Available from: <http://www.canlii.org/yk/laws/sta/78/20060728/whole.html> [cited 2006 Nov 2].
- 66) Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c. 20. Available from: <http://www.canlii.org/nt/laws/sta/1994c.20/20060718/whole.html> [cited 2006 Nov 2]. Enabled regulation: Access to Information and Protection of Privacy Regulations, N.W.T. Reg. 206-96; in force: 1996 Dec 31.
- 67) Access to Information and Protection of Privacy Regulations, N.W.T. Reg. 206-96. Available from: <http://www.canlii.org/nt/laws/regu/1996r.206/20060718/whole.html> [cited 2006 Nov 2]. Enabling statute: Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c. 20; in force: 1996 Dec 31.
- 68) Hospital Insurance and Health and Social Services Administration Act, S.N.W.T. 1988, c. T-3. Available from: <http://www.canlii.org/nt/laws/sta/t-3/20060718/whole.html> [cited 2006 Nov 2].
- 69) Hospital and Health Care Facility Standards Regulations, N.W.T. Reg. 036-2005. Available from: <http://www.canlii.org/nt/laws/regu/2005r.036/20060718/whole.html> [cited 2006 Nov 2].
- 70) Evidence Act, R.S.N.W.T. 1988, c. E-8. Available from: <http://www.canlii.org/nt/laws/sta/e-8/20060718/whole.html> [cited 2006 Nov 2].

- 71) Canadian Medication Incident Reporting and Prevention System: CMIRPS core data set for individual practitioner reporting. Toronto (ON): Institute for Safe Medication Practices Canada; ©2001-2006 [cited 2007 Mar 8]. p. 24-25. Available from: <http://www.ismpcanada.org/download/CMIRPS%20Core%20Data%20Set%20for%20Individual%20Practitioner%20Reporting%20April%202006%20ISMP%20Canada.pdf>
- 72) A medication incident reporting and prevention system for Canada: business plan. City: Canadian Coalition on Medication Incident Reporting and Prevention; DATE. Available from: <http://www.hc-sc.gc.ca/hpfb-dgpsa/tpd-dpt/cmirms> [cited 2007 Mar 17]
- 73) Manufacturer and User Facility Device Experience Database (MAUDE). Available from: <http://www.fda.gov/cdrh/maude.html> and <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/search.cfm> [cited 2007 Mar 17].
- 74) Code of Federal Regulations – Title 21 – Food and drugs. Rockville (MD): Food and Drug Administration (US). Available from: <http://www.fda.gov/cdrh/aboutcfr.html> [cited 2007 Mar 17].
- 75) World Alliance for Patient Safety. WHO draft guidelines for adverse event reporting and learning systems: From information to action. WHO/EIP/SPO/QPS/05.3. Geneva (Switzerland): World Health Organization; 2005 [cited 2007 Dec 10]. Available from: http://www.who.int/patientsafety/events/05/Reporting_Guidelines.pdf

This project is
partially
funded by:



Striking a Balance: Facilitating Access
to Patient Safety Data While Protecting
Privacy Through Creation of a National
Harmonized Standard

Investigators:
Weisbaum et al., 2007