

Plenary Session 3: Health Information Privacy and Public Health System Needs: Can They Coexist?

Moderator: Jean-François Luc

Director, Policy and Partnerships Division, Public Health Agency of Canada

Session moderator Jean-François Luc, Director of the Public Health Agency of Canada's Policy and Partnerships Division, stated that "information is to public health surveillance what a scalpel is to a surgeon." He noted that the past decade "has seen a proliferation of laws, regulations, guidelines, policies, and procedures that seek to control the manner in which we collect, use, retain, and dispose of information."

Manuela Di Re

Health Law Counsel, Information and Privacy Commissioner of Ontario

Manuela Di Re, Health Law Counsel with the Information and Privacy Commissioner of Ontario, said the increased electronic transfer of personal health information has made privacy protection more important than ever before. "It's not just about primary delivery of health care," she said. "Personal health information is being used increasingly for secondary purposes, such as research, planning, surveillance." While "all of these are equally laudable goals," experiences ranging from the SARS outbreak to the HIV/AIDS epidemic show that individuals and groups can face discrimination and stigma following the release of health information.

The fear of discrimination can undermine public trust and confidence in the health care system, Ms. Di Re said. One study in California found that one in six Americans take steps to protect their personal health status by declining to seek information, testing, or treatment, or even by falsifying records. In Canada, an estimated 1.2 million people have withheld health information because of privacy concerns, and more than 700,000 have declined to seek treatment.

Although the Canadian Charter of Rights and Freedoms protects the privacy of health information, Ms. Di Re said the protection is not absolute. "As with every Charter right, it's balanced," she said. "The right of privacy of the individual is balanced against the public interest." In common law, privacy might be protected by provisions against negligence, breach of fiduciary duty, nuisance, trespass, defamation, and assault or battery. Key professions recognize an ethical duty to protect confidentiality, and there has been a proliferation of privacy and access to information legislation at the federal and provincial/territorial levels.

Ms. Di Re drew a series of themes from the dozens of laws in force, including:

- Information must be collected directly from the individual, unless that person authorizes third-party disclosure, or the information-gathering is permitted or required by law.
- Information must only be used for purposes to which the individual has consented, or for a purpose that is permitted or required by law.
- Information can be disclosed, with or without consent, to avert or minimize danger to any individual or to comply with a court order, or when disclosure is permitted or required by law.

In putting these principles into practice, Ms. Di Re said, the first question is whether the interest of protecting public health outweighs the infringement of individual privacy. In the aftermath of the SARS outbreak, the Information and Privacy Commissioner of Ontario produced a fact sheet on emergency disclosure, after realizing that health care providers were unclear on the laws governing public health disclosure. She said practitioners must also consider:

- Whether obtaining consent is impractical, or would defeat a legitimate public health objective;
- Whether the disclosure infringes on personal privacy to the minimum extent possible to achieve the public health objective;
- Whether the disclosure will be effective in achieving the objective;
- Whether alternative approaches are available;
- Whether information has been aggregated and identities have been protected to the extent possible;
- Whether access to personal information has been limited to those who need to know.

Frank Work

Information and Privacy Commissioner, Alberta

Frank Work, QC, Information and Privacy Commissioner of Alberta, warned participants that “I’m not sure if you and I can be good friends. Your cause is too good, your motives are too pure, and it’s too hard for me to argue against public health surveillance or to argue that privacy is a trump card.” From a privacy point of view, the problem is that too many societal imperatives have trump cards to play—from security against terrorism, to research to cure cancer, to the convenience of loyalty cards, to school surveillance that might save a child’s life.

In Alberta, the 1998 *Health Information Act* treats health care providers as information custodians. The comprehensiveness of the law motivated one prominent lawyer to describe it as an expropriation of Albertans’ health information, which placed the Commissioner in the position of receiving stolen goods. The purpose of the law was to facilitate the development of electronic health records, and the trade-off was the creation of a commissioner’s position to supervise the collection and use of personal information.

“The imperative, privacy, got trumped,” Mr. Work said. “It wasn’t a total rout. There were some rights and guidelines established. But it was very much a matter of the removal of a large degree of individual control over health information for a greater

public good.” The experience underscored the extent to which the public will accept infringements on privacy in the interest of the benefits public health can offer. “At the end of the day, you’re going to be able to get just about anything you want out of those laws,” he told participants. “And therefore you need to tread lightly, because people are going to be relying on you.”

A key feature of the Alberta *Act* is its requirement for privacy impact assessments for all electronic systems—from a provincial cancer board, to a general practitioner’s office—involved in collecting, storing, using, or disclosing health information. With only 1,000 assessments complete, Mr. Work said there are many more to follow. But a deeper concern is that the systems are being developed incrementally, without the kind of planning and forethought that should be devoted to health records or to public health surveillance.

The same incremental approach is being applied to security-related information systems, where the fear of terrorism or crime is leading toward broad data mining techniques to identify potential threats. Mr. Work said the design of public health information systems should reflect the following questions:

- What information is being collected? Is it the minimum needed, and is it accurate?
- Why is the information n being collected?
- What are the other possible uses for the information? How will requests from research, law enforcement, or security authorities be handled, and who is in charge?
- To whom will the information be exposed?
- Is the system secure?
- Will custodianship be outsourced, and will due diligence be assured?

Mr. Work said the Alberta legislation contains two important override provisions requiring information custodians to collect, use, and disclose information with the highest possible degree of anonymity, and to confine their activities to the least amount of information that is required for a given purpose. But “those are particularly hard to enforce in a health care scenario, because who knows what is relevant?” Ultimately, he said, the decision relies on the good will of the practitioner.

The biggest risk with privacy impact assessments is the potential for “function creep,” particularly when an organization fails to designate a lead contact for its database. Researchers, followed by law enforcement and security, are bound to see the database as a valuable source of information, so “these things have to be thought out in advance,” Mr. Work said. He added that health information held on portable computers must always be encrypted: “We’ve had more laptops disappear lately, and locking it in your soft-top Jeep is not an acceptable security measure.”

Elaine Gibson

Associate Director, Health Law Institute, Dalhousie University, Halifax, NS

Elaine Gibson, Associate Director of the Health Law Institute at Dalhousie University, agreed that public health can make a compelling case for access to health information. Information sources are clinical in the first instance, but administrative databases compiled since the 1970s “are now very potent sources of information, especially in Canada because of our universal Medicare system.” Electronic health records, as well, “are very, very powerful sources of information, in the first instance for clinical purposes, but now for research and surveillance.”

Ms. Gibson distinguished between the nominal versus non-nominal, identifiable or not, anonymized, and aggregate health data that might be released under different circumstances. “These have gradations of privacy interest,” she said. “We now recognize that these are relative terms. It’s not that information is either identifiable or not. Especially when it comes to databases and combining databases, each piece of information has a degree of identifiability in the circumstances.” Aggregate data provides the highest degree of comfort from a privacy standpoint.

A key concern identified by the Naylor Committee report on the 2003 SARS outbreak was the existence of separate public health surveillance systems in every province and territory, alongside a federal system operating mainly at Canada’s international border. This structure goes back to the constitutional division of powers. Ms. Gibson said federal powers may be invoked in relation to criminal law, areas of national concern or emergency, or the federal mandate for peace, order, and good government. But she said the Supreme Court has attached a fairly narrow definition to areas of national concern, and the scope of an emergency is clearly limited.

Authority to collect information crosses jurisdictions, as well, she noted. The federal government has authority for census and statistics, and its jurisdiction over trade and commerce gives it responsibility for the *Personal Information Protection and Electronic Documents Act* (PIPEDA). But Quebec has launched a constitutional challenge against PIPEDA, and the provinces have authority over property and civil rights and matters of a local or private nature.

In 1999, this patchwork of legislative authorities led the Auditor General to criticize weaknesses in the national public health surveillance system, including the lack of a clear obligation for provinces to report communicable diseases to the federal government or other provinces and territories. Ms. Gibson said some provincial legislation is silent on reporting, while other statutes permit but do not require it. The only province with mandatory monthly reporting is Prince Edward Island, but she said local authorities are not always aware of the requirement. More broadly, she stressed that laws can facilitate, impede, or protect public health, “and if the balance isn’t right, we have to get it right.” That obligation is reinforced at the international level. Ms. Gibson said PIPEDA was motivated by a European Union decision to stop trading information with countries that failed to offer a reasonable level of protection. Canada also faces pressures from sources as diverse as the U.S. *Patriot Act*, the World Health Organization, and the Organization for Economic Co-operation and Development (OECD), which adopted a declaration on sharing of information for research purposes in 2004.

She said federal and provincial/territorial governments are well on the way to developing collaborative information-sharing agreements, and that harmonization of provincial/territorial legislation may also be a possibility. There has also been some discussion of new federal legislation for information-handling that would “make much more explicit for the federal government what uses they can make of the information.”

Questions and Discussion

A participant said there is “massive under-reporting” of public health data by practitioners and institutions, but noted that the same information can be gathered elsewhere—for example, pharmacy databases track sentinel drugs that are indicative of the spread of infectious disease. He asked whether similar data sources are available for non-communicable disease, and whether there is a point where privacy concerns outweigh the need for better public health data.

Ms. Gibson said those issues, including the need for consent, are addressed when legislation is drafted. “On the other hand, I would not say that public health has necessarily been foremost in the minds of the drafters.” She added that privacy does take priority at some point, but “we’re not exactly sure when, because we have few court cases—especially higher court cases—that deal specifically with information and public health.”

Mr. Work agreed that exemptions in existing legislation already permit public health surveillance. “The vehicle is there,” he said. “It’s just being driven in 13 rather different ways, and that’s problematic for both the public health side and the privacy side.” Ms. Di Re said Ontario’s health information privacy act contains a broad exemption in favour of health protection and promotion, but health practitioners are still reluctant to disclose information in situations where they would be able to.

A participant invited the panel to comment on health information and privacy in Canada’s 600 First Nations communities. Mr. Work recalled that First Nations had been reticent to release information the federal government wanted to collect in connection with benefit payments, but that could be used for other purposes. Ms. Gibson noted that the National Aboriginal Health Organization had taken the “very interesting step” of asserting ownership over First Nations’ health information.

A participant asked how PIPEDA would affect cancer surveillance when the legislation is intended to serve commercial purposes. Ms. Gibson said the definition of commercial activity is based not on the nature of the organization, but on the actual activity where the information is being collected, used, disclosed, and maintained. Industry Canada has exempted hospitals from PIPEDA as non-profit institutions, but has included private practices and laboratories that operate at a profit. The courts have not yet ruled on the matter, she said, and “I’ll be surprised if what Industry Canada says is the last word on the subject.”

Recalling Mr. Work's statement that it is difficult to turn down access applications that seem motivated by good intentions, a participant asked whether questions of privacy and ethics should be linked with a review of methodology. Mr. Work said it would be fascinating to see a checklist of the necessities for a public health surveillance system. "If privacy people knew what public health needed or had to have, then we could have that argument," he said. "But I have yet to see the template for what a good, viable public health surveillance system requires."