Ensuring Privacy and Confidentiality on Canada's Health Iway

CANARIE INC.

December 1997

Table of Contents

Preface

This is the third in a series of reports issued by CANARIE Inc. on telehealth in Canada, and is based on a workshop held in St. John's, Newfoundland in October 1997, entitled *Ensuring Privacy and Confidentiality on Canada's Health Iway.* The workshop brought together more than 70 stakeholders from the health community, government and the private sector to identify policy, legal, regulatory and technological issues, solutions and clinical protocols relating to privacy, confidentiality and security in telehealth in Canada.

The first CANARIE report, *Towards a Canadian Health Iway: Vision, Opportunities and Future Steps*, released in September 1996, set out a vision of a Canadian Health Information Network — the Canadian Health Iway — and recommended several follow-up actions. The reports of other groups echoed these recommendations, and collectively helped create a broader awareness of the strategic importance of telehealth in Canada.

CANARIE released the second report in July 1997. *Telehealth in Canada: Clinical Networking, Eliminating Distances* was based on a CANARIE workshop held in Quebec City in March 1997. Participants from across Canada focussed on new applications of telehealth, the latest developments by governments and the private sector, and the challenges on the road ahead.

The Canadian Health Information Network Vision

The Canadian Health Iway will be a virtual information centre, created and used by communities and individuals across Canada. It will be open and accessible, yet feature sufficient confidentiality and privacy to assist decision making by health professionals and patients; it will support research and training and facilitate management of the health system; and it will respond to the health information needs of the public. The Canadian Health Iway will be an agent of change for the health system, contribute to improving the health of Canadians, and foster the development of globally competitive Canadian technologies and services.

This third CANARIE report is not intended to be a comprehensive treatment of the subjects of privacy, security and confidentiality. Nor does it represent the personal perspective on these issues of any single author. Rather, it is simply a report on the discussions of these matters that took place at the St. John's workshop. Although the contributions of many participants are reflected, the bulk of the report features no direct attribution. Further background regarding CANARIE's telehealth activities can be found at CANARIE's web site (*www.canarie.ca*).

Introduction

The Opportunity

In 1901, atop Signal Hill in St. John's, Newfoundland, Guglielmo Marconi received the first transatlantic wireless transmission from Cambridge, England. This spirit of innovation is also found in modern-day pioneers in Newfoundland, who apply information and communications technology (ICT) in innovative ways to address the special challenges imposed by Newfoundland's rugged geography and thinly distributed population.

Telehealth, or the application of ICT to health, has long been of special concern to Newfoundlanders. Lieutenant-governor Dr. Max House, himself a pioneer in this field, sees telehealth as a matter of making *intelligent connections* to improve health outcomes. Many innovations in the use of technology in health delivery have arisen from the activities of Dr. House and his colleagues in Newfoundland.

The state of telehealth in Canada as a whole is similar to that in Newfoundland. Moreover, with its strengths in the ICT sector, and the strength of its universal health system, Canada appears poised to become a leader in the development of innovative applications of ICT to health.

If this is to happen, provincial governments must play a critical role. Driven by pressures to lower costs, become more efficient and deliver high quality services to remote regions, many provinces are accelerating the development of telehealth applications. ICT can help eliminate duplicate medical records, reduce the reordering of tests, and prevent patients from taking multiple prescription drugs that negatively interact with each other. As a result, provincial ministries of health are becoming very aggressive in reforming and streamlining their information systems.

Applications beyond reformed information systems hold equal promise. Network-enabled consultations, for example, allow physicians in remote regions to consult with specialists in urban health centres, improving access to health services for patients while eliminating the need for costly and time-consuming travel.

Improved links among health information resources through computer networks can assist in the general movement in the health field toward *evidence-based decision making* — establishing more effective procedures through the systematic collection and analysis of treatment and research data. The National Forum on Health recently recommended adopting such an evidence-based system, and defined it as "the systematic application of the best available evidence to the evaluation of options and to decision making in clinical, management and policy settings."

Perhaps the best way to improve health over the longer term, of course, may be to provide the information people need to take charge of their own health. The National Forum on Health stressed the urgent need to shift the emphasis away from health care and toward the broader concept of health itself, including key determinants of health, such as socioeconomic conditions and education about healthy lifestyles. Again, ICT and telehealth would appear to be elements of the solution to this challenge.

Telehealth can contribute to all these applications — from improved health information systems and remote consultations and related services, to evidenced-based care and better consumer health information services. The consensus has developed in the health community that, within this mix of applications and approaches, there lies a wealth of benefits that will only be realized through the creative application of ICT. The challenges that must be overcome are numerous, of course, and some may prove to be especially troubling, perhaps none more so than the debate over privacy and confidentiality.

The Threat

Privacy and confidentiality are not new concerns in the health field. Indeed, the confidentiality of patient-physician exchanges has a legal and philosophical foundation developed over many years. Nonetheless, the use of powerful information systems and the linking of those systems through advanced networks add new layers of complexity, if not risk.

Some observers contest the claim that new technology adds risk, pointing out that the ideal of full protection of personal information is far from being met by current, paper-based practices, and contending that advanced information systems may actually offer a more secure environment for sensitive data. They point to the fact that, today, an estimated 70 per cent of violations of this sort involve trusted insiders in the health system, and that improved security technology will prevent many of these people from having the kind of unfettered access that the current paper system provides. In short, the technology might actually be the saviour of data protection in health, not a threat to it.

Whatever the merits of this view, public consciousness of privacy and confidentiality in health has grown over the past decade, and has proven to be a very compelling issue for many Canadians. In surveys about the Information Highway, privacy has been cited time and again as a top area of concern.

As a result, the media have made privacy a recurring theme, frequently focussing on fear-provoking stories about security breeches on the Internet, for example. In a world of networked information, the danger scenario is easy to paint: hackers altering health records just for fun; corporations stealing records to better target potential customers; or, worse yet, insurance companies or employers accessing an individual's private health information to his or her detriment.

While these scenarios can be easily exaggerated, behind them lie the undeniable truths that personal health records contain information that can be exploited by others and that abuse of network access is a definite possibility. Paradoxically, the real threat may not result from the new technologies making personal data inherently more accessible, but from the potential value to others once the data have been collected and stored in one place for legitimate purposes.

There is more to this than just hacking and theft, of course. Being protected against the sale of personal health records, valuable in their own right, is another possible, perhaps even greater, concern. Certainly, it is one of the fears many people have as private-sector thinking and private-sector organizations come to dominate Canada's health system.

Adopting highly advanced encryption systems will likely alleviate many of the Internet's security problems. Still, public perceptions that data are not safe may undermine public confidence and trust in health information networks. Most people take the privacy of their health information for granted. But, a security breech in one province, perhaps one that is a leader in health networking, could lead to such extensive media coverage that it undermines the efforts of all other provinces, simply due to the devastating impact on public perceptions. There may be no way to fully protect against such an eventuality. However, since the risk is shared, there would appear to be a compelling argument for a broad-based cooperative effort to minimize that risk. There will likely be no second chance to restore public confidence if a serious breech were to occur anywhere in the country.

Properly addressing privacy, confidentiality and security in telehealth is clearly one of the most important challenges to the successful development of Canada's health information network. As noted by the Privacy Commissioner's *1997 Annual Report*, "a Canadian health information system could either stand or fall on the extent to which it incorporates privacy, patient autonomy and informed consent."

Definitions

Individual Canadians have differing views about privacy. Some see the information collection activities of governments, or even the private sector, as largely benign. Others distrust such activities, favouring maximum privacy protection. Lying behind these views are different experiences and perhaps different levels of understanding. Confounding this situation, and often impeding effective dialogue, is that people use key terms in varying ways, and blur important distinctions.

Privacy, Confidentiality and Security

Privacy, confidentiality and security are terms that are clearly related, but that mean quite different things. While there is no universally accepted set of definitions, a broad consensus supports the following[1]:

Privacy A right of an individual arising from the values of individual autonomy, freedom and dignity. It can be defined as the right to be left alone, remain anonymous and free from intrusion; to control information about oneself; to withdraw from the influences of the environment; and to be protected against physical or psychological invasion, or against the misuse or abuse of something one legally owns or that is normally considered by society to be one's property. In the context of the St. John's workshop, the term privacy was used largely to refer to "personal data protection," although the term clearly has a broader meaning.

Confidentiality A property of information which, when conferred, mandates that access to that information should be controlled, and that it is incumbent on those controlling access to the information to closely monitor and strictly limit access and disclosure. Confidentiality can mean choosing to provide information, but expecting that it be kept secret.

Security The set of safeguards in and around an information system that protect access to the system and the information it contains. Security measures include the hardware, software, personnel policies, information practice policies and disaster preparedness relating to the information system, as well as oversight processes in all of these areas. The purpose of security is to protect the system and the information it contains from unauthorized access and abuse, both from without and from within.

Relationship: Good security is essential to confidentiality but does not guarantee it; good security and confidentiality are essential to protecting private information but do not guarantee it; full protection of private information is essential to full privacy protection.

---

[1] See definitions in a background paper by Andrea Neill at *www.canarie.ca/eng/outreach/health/back*. Another good source is *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality* by the Center for Democracy and Technology in Washington, D.C.

Access, Ownership and Control

As might be expected in any debate about moral or ethical issues, clear definitions do not settle the matter. For example, definitions alone do not resolve the issue of when it might be legitimate for an individual's right to control access to their personal health information to be overridden. Clearly, a health professional should not simply be able to assert a "need to know" in order to gain unauthorized access to private information. The health profession requires specific guidelines, (in fact, many jurisdictions have already developed them), that set out in detail what "need to know" and "legitimate access" mean in practice.

Patients have a fundamental right to access their own medical records. Therefore, a patient's doctor, or anyone else that is specifically authorized by the patient, should have access as well. Moreover, most Canadians would want to ensure that the right information is made available to the physician treating them in an emergency situation, so some form of access that the patient does not authorize should be permitted. Beyond that point, however, it is less clear how to proceed.

Approaching this matter from the perspective of *ownership* of information might offer some assistance. It might be argued, for example, that patients are the owners of any and all personal health information pertaining to them. This would seem to be undeniable, and could be taken as a legitimate starting point for unravelling the complexities of access and control; however, even here there are debates. For example, when a patient sees a physician, it is the physician who creates the record of the visit, not the patient. In some instances, when diagnosis and treatment are unclear, the records of an extended series of appointments might feature considerable analysis, including the physician's hypotheses and conjectures while attempting to make a diagnosis. In particularly challenging cases, the physician's path of inquiry can lead to discoveries, which in turn can lead to certain intellectual property being developed.

Currently, the right to exploit that intellectual property, through publication for example, belongs to the physician, so those portions of the medical record that contain the physician's observations of the symptoms and conditions presented by the patient and the ongoing enquiry into their cause would seem to be the property of the physician, not the patient. Perhaps a deeper discussion of ownership over the records of patient-physician encounters is needed.

The issue of control over access to information has already been mentioned. Traditionally, control over access rests in the hands of the attending physician. But if ownership of information rests largely or as least partly with the patient, then control over access, or at least control over access for purposes other than that for which the information was collected, should rest with the patient.

The purpose of this report is neither to settle any of these moral, ethical or legal issues, nor to summarize the effort that has been put into addressing them over recent years. That patient health information has value, that it can be owned and sold, and that different but related pieces of information may be owned by different participants, all seem to be fundamental propositions related to the issue of access and control. Those issues, moreover, would seem to be central to the debate that must occur to develop a consensus for action on telehealth.

Data Types

A third matter that provides an important foundation for the discussion of access to personal information concerns the term data itself. Health data can be classified as follows:

non-identifiable	data that cannot be linked back to a particular individual;
coded	data that, with effort or if other information is possessed, could identify an individual; and
personal	data that identifies an individual.

Non-identifiable data (e.g. aggregated data) generally do not pose a problem, since any identifying features are stripped away. Nevertheless, some possible concerns arise. For example, aggregated data regarding the prevalence of a disease in a particular town, or in any identifiable segment of the population, could lead to discrimination against individuals from that town or in the defined group (e.g. insurance rates for First Nations). Also, insufficiently aggregated data could result in the identification of individuals. (The *Statistics Act* provides a guide for addressing the latter situation. For example, Statistics Canada cannot publish survey results if there are fewer than five people in thesample.)

Data that can be associated with a particular person should have the most protection. As noted above, protection of private information is a "right," and a legislative framework, developed by the federal and provincial governments, is part of the means of protecting that right.

A Stakeholder Framework

Beyond the office itself, information transfer on an electronic network leads to other potential security threats. In the near future, all personal health information sent across a network will have to be encoded at source, perhaps including "public key" encryption techniques

As outlined above, the issue of protecting access to private information in a networked world is no different than it is in a largely paper-based world. The issue comes down to striking a balance between the benefits that follow from improving access by certain individuals to certain information in certain situations and the risk that abuse will take place if information is too readily accessible.

One effective strategy for understanding and dealing with the complexities of striking this balance might be a framework of key stakeholders or potential users of health information. Within such a framework, each stakeholder's needs or uses could be examined, the risks defined and strategies for protection identified. The key questions would seem to include the following: Who owns the data? Who controls its use? How does one protect access in that context against unauthorized access?

Developing comprehensive answers to these questions for all potential stakeholders is beyond the scope of this report. What follows is a preliminary discussion of some of the elements that a framework might contain.

Physicians

Where and how health information is collected has a ripple effect throughout the entire system. The starting point for most data collection is physicians' offices and hospitals, for these are the places where patients interface with the health system. Procedures and protocols at this level are critically important, since all other stakeholders — researchers, administrators and policy makers — are secondary users of information gathered here.

A physician's office has a measure of physical security. A locked door, for example, prevents access by most casual

intruders. Inside the office, however, unauthorized access to information is a major concern even today, since personal health information is readily available to nurses and clerical staff, and potentially to other workers who share the office space or service it. With computer systems, additional physical security usually focusses on protecting the terminal or data-entry system with a password, or perhaps including new features such as a time out for when the user is away from the desk for a period of time or some form of biometric user identifier, such as a fingerprint, hand or iris scan.

Beyond the office itself, information transfer on an electronic network leads to other potential security threats. In the near future, all personal health information sent across a network will have to be encoded at source, perhaps including "public key" encryption techniques (see page 22).

Hospitals, clinics and other related settings may pose a greater security challenge than physician's offices, since a broader array of people potentially have access to a patient's health information, including other physicians, consultants, nurses, technicians, clerical staff and archivists. In today's busy hospitals there is considerable scope for illegitimate access to patients' charts and other confidential information.

Remote consultations pose additional challenges too, especially involving patient consent. During a remote consultation over a network, it may not always be clear to the patient when other observers are in the room with the consulting physician. Such people may include technical staff, informatics experts, medical students, and possibly journalists. Such situations are not the norm, and guidelines are usually in place to protect against them, but they may arise inadvertently so care must always be taken.

As with all transfers of sensitive data over networks, interception of a remote consultation during transmission poses another problem. The sensitive information included in the transmission could include patients' past medical history, lifestyle, habits, sexual orientation, family history and symptoms, the physical examination itself (on camera), laboratory results, medical images and the diagnosis and discussion of prognosis. Many facilities also record such sessions, and need guidelines on when such recording is allowed, who stores the record, who is responsible for security, and how long the record will be archived.

In light of these issues, Dr. André Lacroix underscores the need to reaffirm the fact that health professionals and institutions at a distance share the same obligations to insure confidentiality and the protection of personal data as those in traditional settings. He also recommends national standards or guidelines to ensure privacy and confidentiality in telehealth applications, and technical standards to ensure the security of the patients' electronic charts.

Compared to traditional patient encounters, remote consultations require more caution and stronger measures — through procedures, protocols, guidelines and technical applications — to ensure patient privacy and respect confidentiality. Solutions at all levels must take into account the unique features of telehealth.

Researchers

Researchers are another key stakeholder group. They can contribute to development of evidence-based decision making based on access to health information. Researchers usually only deal with data that have been aggregated and are non-identifiable. However, if individuals are judged to own their own health information no matter

for what purpose, and even if it is aggregated, researchers must obtain consent to use it. Patient consent should include permission to use personal information for evidence-based research, provided the patient data are non-identifiable. Such consent should also specify that the use of the data is for health purposes only.

Given the concern over providing open access to aggregated health information, one protective measure may be to give access to researchers through some type of third-party custodian.

Administrators and Policy Makers

It is rare for administrators to have access to personally identifiable data, so the primary concern for this group may arise not in connection with access to *patient* data, but rather with *physician* data.

Access to health information by administrators and policy makers is necessary to ensure accountability in the system, as well as for billing and financial reasons. Nonetheless, potential abuses are possible. One concern arises in connection with the physician's thinking that eventually leads to a diagnosis. The initial hypothesis may prove to be incorrect, but the thinking process and the reasons for it are an important part of the health record. Use of the records for administrative and policy purposes should respect the need for this kind of evolutionary process.

This tension between the physician's personal information regarding a patient and the need for auditing and oversight poses some challenges. To what extent does the physician's "train of thought" represent his or her intellectual property, and should it even be part of the record that is available to administrators? How much of these thoughts should be put in the "official" record to begin with? To what extent will retroactive liability become an issue in cases in which competing hypotheses are part of an ongoing scientific controversy of which administrators may be only dimly aware?

As with researchers, administrators and policy makers who only deal with non-identifiable data should not pose a threat to patient data. However, access to personal information by a health minister, either regarding a physician or a patient, does remain a concern in the minds of many. There are numerous precedents, some fairly recent, in which an official who should know better made public personal information regarding a patient or physician. There is clearly a need for better understanding of what confidentiality means at all levels.

Patients and Consumers

Currently, patients have access to their medical records, laboratory results and medical images guaranteed by law. Such access, including access to electronic records, would appear to be a fundamental right linked to the right to privacy. More practically, access should also include the right to correct errors in the record. The process for accessing and correcting such information needs to be made clear.

SmartCards are a new technology that will allow individuals a greater degree of control over their health records, since the computer chips embedded in the cards will actually contain the relevant health information. This technology is being introduced by the Quebec Ministry of

Health, and is being considered by others, as a means of improving administrative efficiency. Although the technology could be a powerful tool for the protection of personal data, there is also the risk of loss or theft. Clearly, effective provisions should be made to protect privacy even in such extreme situations.

As always, the desire of people to have control over their personal health information must be balanced against the societal good that comes from sharing some of the information. As noted above, however, issues of ownership and co-ownership of information created by the doctor-patient relationship require clarification. There may also be varying requirements for protection of information, so that patients with AIDS, for example, can have more stringent control if they desire it.

Individuals will also likely have access to aggregated data in some form. While most citizens would not be interested in sifting through such raw data, they may become consumers of health education products based on such data produced by intermediaries. Indeed, the market for consumer health information, to make better lifestyle choices or to perform a self-diagnosis for simple conditions, appears to have promising future.

Toward Solutions

Confidentiality in health matters is well established in Canada through numerous laws and regulations, and through codes of ethics administered by professional bodies such as the College of Physicians and Surgeons.

There is no single set of laws or technological solutions to the challenges raised above. It is truly a matter of "managing the messiness," and taking into account the interrelationships across several dimensions: legislative/policy, technological and behavioural. These elements define a toolkit that makes up an "infrastructure" of technology, people, process, decision making and partnerships.

Two ingredients of a successful approach to these matters are the harmonization and integration of different components of the toolkit. There is a need to develop an effective link between technology and policy, for example. At the core is the need to define "trust relationships" among the different parties in the health system.

Governments appear to be ready to engage on these issues, although jurisdictional conflicts may arise as provinces actually implement health information networks. Instilling a sense of public confidence in the health information system requires coordination among stakeholders in different provinces and institutions, both public and private, as well as at the federal level. Moreover, a balance must be struck between harmonization and flexibility if the particular needs of different jurisdictions are to be met.

Legislative Remedies

Privacy protection in Canada is a shared jurisdiction between the federal government and the provinces. A patchwork of laws, regulations, policies and voluntary measures apply to privacy in the context of the Health Iway.[2]

Federally, the Criminal Code applies to privacy matters, and the *Privacy Act* covers general privacy protection in the public sector. A number of Supreme Court rulings contain key decisions with regard to privacy. *The Charter of Rights and Freedoms*, while not explicitly providing for an individual's right to privacy, has also been cited in a number of Supreme Court decisions, and privacy rights under the Charter appears to be an evolving area of law.

The federal government announced in 1996 that legislation will be brought forward jointly by the ministers of industry and justice to extend data protection to the private sector. However, this will apply only to areas of federal jurisdiction, leaving a sizable gap that must be filled by provincial legislation.

Most provinces have privacy laws for the public sector, although Quebec is currently the only province to have a comprehensive data protection regime for both public and private sectors. Newfoundland, New Brunswick and Prince Edward Island do not have general statutes on public sector data protection.

Confidentiality in health matters is well established in Canada through numerous laws and regulations, and through codes of ethics administered by professional bodies such as the College of Physicians and Surgeons. Quebec's civil law system also protects medical secrecy, and jurisprudence in that province has confirmed that medical secrecy is a right. Manitoba has recently passed legislation that provides a comprehensive framework for the protection of health information with an electronic environment in mind. Alberta has tabled similar legislation.

Privacy Principles

A core consideration in the development of legislation, policies and guidelines regarding data protection and confidentiality is emphasizing the "use" of information, not the "user." For example, health professionals should assure patients that personal health information will be used only for health purposes, and not for secondary or unspecified ones, and that the information will not be sold. Needless to say, these principles must be accompanied by provisions for auditing and enforcement.

Building on the principle of an individual's control over their own health information, a set of core principles regarding practices for collection, storage and dissemination of information should be developed. An excellent starting point for such a set of principles is the Canadian Standards Association's (CSA) *Model Code for the Protection of Personal Information*, a Canadian voluntary code developed in response to the need for a harmonized approach to data protection. The Code is based on the *Guidelines on the Protection and Trans-border Flows of Personal Data*, published by the Organisation for Economic Cooperation and Development, to which Canada subscribed in 1984.

The Code serves as a useful guide for a framework of privacy protection in the area of telehealth. The Information Highway Advisory Council, in its Phase 1 *Final Report*, endorsed the CSA principles, recommending that "the federal government should act to ensure privacy protection

---

[2] What follows is a summarized version of material presented at the workshop by Andrea Neill of the Department of Justice. For a more detailed presentation, please refer to Ms. Neill's background paper, *Legislative and Regulatory Strategies for Canada*, available on the CANARIE Web site (*www.canarie.ca/eng/outreach/health/back*).

on the Information Highway. This protection shall embody all principles of fair information practices contained in the CSA draft *Model Code for the Protection of Personal Information*."

The CSA code sets out 10 principles:

Accountability — An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Identifying Purposes — The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

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

Limiting Collection — The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Limiting Use, Disclosure and Retention — Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Accuracy — Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

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

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

Individual Access — Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

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

The experiences of other jurisdictions might also be helpful. The United States appears to favour a *laissez-faire* approach, and has much less protection of personal information than Canada has. In its *Directive on Data Protection*, which will come into effect in October 1998, the European Community takes a very different approach: transfer of personal information to other jurisdictions is actually prohibited unless they have a similarly high standard of privacy protection.

Although Canada must set its own course on these issues, it could gain a clear economic advantage by following the European direction. Take, for example, the case of a European company wanting to set up a factory in North America. If Canada were to adopt privacy laws consistent with those of Europe, while the U.S. did not, it would strengthen its case for the company locating its factory here. Limitations on the transfer of personal information, such as customer or personnel information, between the North American and European arms of a multinational organization would constitute an inefficiency that they would want to avoid. Quebec is a model in this regard as its private sector legislation already conforms to European standards.

Protocols and Guidelines

Additional considerations lie beyond the legislative domain. Critical data protection issues are connected with such practical matters as how information is collected, how it is stored and how agents in the system interact, and none of these is likely to be addressed by legislation. At this level, clinical protocols, guidelines and codes of conduct fill in the gaps. Indeed, as noted above, the historical relationship of confidentiality between doctor and patient rests on such mechanisms.

Of particular concern are codes of conduct and practice guidelines that address ownership of information, transmission of information and harmonization across jurisdictions. There will be several levels in the health system at which these matters arise and guidelines will be needed: professional, in the interaction with private sector organizations, and within government itself, for example.

In the development of these guidelines and protocols, it is increasingly important that private sector organizations be involved, as in many cases they will be the developers and implementers of solutions. Ontario's Project Management Office, for example, includes private sector partners.

One approach to the development of guidelines might be to elaborate the stakeholder framework outlined above and address a set of interrelated questions: What information can be shared? With whom? For what purposes and under what conditions? What are the risks faced by different stakeholders? What are the strategies for mitigating that risk? In one sense, such a study might constitute a risk-minimization exercise in connection with the possibility of a major breech in security affecting individual privacy. Cost considerations are also a factor in developing such risk analyses or assessments. The Canadian Institute for Health Information has done preliminary work in this area and is poised to undertake more.

Other key considerations in developing such frameworks are auditing, accreditation and accountability, in particular independent auditing and accreditation. The sharing of security responsibility and the role of contractual relationships, such as bonded contractors, are other related matters.

Existing oversight mechanisms may provide instructive models and help clarify roles. One example is the role played by Health Care Facilities Accreditation Bodies. Such oversight and accreditation mechanisms might perform a useful role with respect to the security of networks or public key infrastructure security-level classifications, for example. Most public institutions, such as hospitals and universities, also have independent auditors assessing security issues relating to data processing activities, and security-level classifications might soon be taken up in those forums. Of course, at some point auditing can become overly intrusive and counterproductive, much as too much surveillance in the workplace can have a negative effect on employee morale.

Moving Forward

The principles of the CSA Code serve as a basis for legislation, but it is unclear whether there needs to be federal legislation (e.g. a national health informationprotection act) in addition to provincial legislation, or whether a policy framework of principles would suffice. There is general agreement that legislation, whether federal or provincial, should not be overly rigid, as the context is evolving too rapidly. Any federal legislation or regulation, of course, must be flexible toward provincial jurisdiction, given the role of the provinces in tailoring their own approaches.

Neill suggests an approach to legislation based on three complementary components:

- *general framework legislation*, adopted at the federal, provincial and territorial levels, that is based on the CSA Code and that sets out binding and fair information principles and rules;
- *specific health information legislation* that sets out rules for the collection, storage, use and disclosure of health data; and
- *supervised self-regulation* in the health sector that consists of policies, procedures and specific health information codes, with internal and external oversight mechanisms.

This approach would seem to have considerable merit.

In the context of health information in an electronic environment, the Privacy Commissioner's *1997 Annual Report* recommends the following measures:

- Enact complementary federal and provincial legislation to protect the privacy of the full range of personally identifiable health care information. The legislation would incorporate the fair information principles of international data protection agreements. This must be done before the health network develops further.

- Establish clear requirements for obtaining the informed consent of patients for disclosures of personal information. In the absence of informed consent, an individual's right to control the disclosure of personal medical information should be paramount. That right should be overruled only in the face of an overwhelming and compelling public interest (or to provide the patient with emergency care). Conducting research does not always constitute an overwhelming or compelling public interest.

- Establish strict limits and controls on the circumstances under which access to personally identifiable information is granted to secondary users for research purposes and encourage the conduct of research through the use of aggregate, depersonalized data.

- Establish strong remedies in law for disclosing information without a patient's consent.

- Educate patients about how their records are used and the privacy implications of having their medical records computerized and placed on a national network.

- Develop guidelines to address the privacy and security issues raised by the computerization of patient data, including provisions for full audit and control.

- Establish an independent review mechanism to oversee the privacy of health care information.

Clearly, and as stated earlier, a balance is needed in any legislative or regulatory framework to protect the right of individuals to privacy but eliminate barriers to information sharing when this is deemed desirable.

Technological Solutions

Various security technologies are rapidly evolving in response to the needs of the health sector and others. The shortcomings of the current, largely paper-based system provide one possible starting point for choosing among the alternatives.

The activities in this area of the banks, travel agents and airlines provide another starting point. Each of these groups operate extensive networks and have security concerns of their own. The federal government has also been developing security technology for its own networks. One important security project of the government relates to the development and implementation of a "public key infrastructure" system, or PKI for short.

Public Key Infrastructure

Technology associated with PKI could have great significance for health.[3] It is a sophisticated form of encryption that can provide a basis for secure communications, and address the need for secure standards in transactions processing and data interchange.

PKI also addresses the need for networks to "break out of the enterprise." Currently, information networks are largely employed at the level of individual enterprises. As use of networked information systems grows, however, interoperability between enterprise systems through external networks becomes essential. From a security perspective, this requires an ability to identify other organizations on the network, be able to confirm who they are, and establish how secure or "trusted" that domain is. Before sending sensitive information to another domain over the network, it must be possible to confirm its security level.

A Primer on PKI

The use of ciphers and codes to protect sensitive information goes back to the days of Julius Caesar. The underlying principles of modern techniques are much the same as they were then, although the advent of computer technology has made their application more sophisticated.

Private, or symmetric, encryption uses a "key" to scramble a message. That message can only be unscrambled using the same key in reverse. The difficulty with symmetric encryption is that to unscramble a message, the recipient must have the key. For keys to be conveyed to each recipient of an encoded message in a secure fashion, another secure way of transmitting them must be devised. For modern global networks, with unlimited numbers of potential recipients of countless encoded messages, the inability to distribute encryption keys in a secure fashion, and the need for there to be different keys for different sets of individuals, and perhaps for different messages, means that the private-key approach simply does not offer a general solution.

A technique called public key encryption solves the problem. This scheme uses two keys to scramble and unscramble messages. The private key is unique to each individual and is kept secret by that individual. The public key for

---

[3] This section owes much credit to Bob Cavanagh, Bill Dziadyk, Ross Fraser, Bob Little and Mike Pluscauskas, who shared their expertise on PKI at the workshop.

that individual is openly accessible to all those wishing to send messages to that individual. The keys are mathematically derived in such a manner that, for Tom to send a message to Brenda, he need only encrypt the message using Brenda's public key, after which it can only be decrypted using Brenda's private key.

Applying this operation in reverse creates a digital signature that proves that a message can, indeed, only have been sent by Brenda. To create a digital signature, Brenda need only encrypt the "signature" she attaches to her message to Tom using her own private key, which can then only be decrypted with her public key. Although anyone can apply this public key, making the signature not a secret, it does prove that the message was sent by Brenda, since only Brenda has access to her private key. This is also called authentication.

To prove that a message has been sent in its entirety and has not been tampered with (called ensuring integrity), a mathematical function is run on the original message to produce a unique number. If running the same hash function on the decrypted message produces the same result, then the content of the message has not been tampered with.

For this system of public and private keys to work in practice, there must be a third party, called a Certification Authority (CA), who assigns private keys and keeps a record of public keys. One of the roles of such an external authority is to avoid a third party, Greg, from masquerading as Brenda and telling Tom that his public key is Brenda's. If Brenda's public key can only be transferred to Tom by the CA, and is digitally signed to authenticate that it was the CA that indeed sent it, then Greg cannot masquerade as Brenda. This is known as obtaining a certificate of authenticity from the CA.

When described on paper the public-key process sounds complicated. Fortunately, most of the back-and-forth activity can be managed transparently by PKI software running on the user's computer. Clearly the security system needs user-friendly interface if PKI is to be adopted.

This ability to establish a level of trust between domains on a network is a key capability of a PKI system. Through the issuing of certificate policies by a certificate authority, levels of security can be defined as a basis for the secure exchange of data, even though the parties making this exchange may not know each other directly. The PKI model being developed by the federal government, for example, defines four levels of security. Certificate policies provide for "classes of activity across communities of interest" that have common security requirements. Such an approach defines a matrix that can be used to establish where each domain lies on the security spectrum — from loose to iron-clad.

In the PKI model, Certification Authorities are decentralized, so that each member of a community of interest can use a common CA. CAs are then connected in a network for transactions that must go outside any one community's CA. In this model, a "Root CA" sits at the top of a hierarchy of CAs. Notably, however, the Root CA cannot derive the private keys of individuals.

Even if a version of PKI was adopted as the foundation for technological solutions to data protection, some issues remain outstanding. One fear is that it will create a bureaucracy, despite the inherent decentralization of the model. Cost is another concern, since the price of the PKI administration rises in proportion to the level of security desired. Tradeoffs may be required if the maximum level of security is prohibitively expensive. This might raise con-

cerns in the health sector, where cost reduction holds sway. While dollars alone will not solve the problem, the issue of how costly PKI will be to implement, and who should pay (the province? the doctor's office? the individual?) are critical to any solution.

Standards Issues

A discussion of security in not complete without a mention of standards. In the information and communications technology (ICT) sector, standards are particularly important, since the growing complexity of computers and networks makes interoperability of different software and hardware components an absolute requirement, in health areas as in all others. Gone are the days when one could build a complete and effective information system using only the products offered by a single vendor.

From the vendors' perspective, standards can often help to create a level playing field for competition in a market, since they define a set of properties, interfaces or operating conditions that, when met, enable any product to interconnect and operate with any other.

Standards can also confer competitive advantage if one market player dominates the setting of the standard. An example of this is the Windows operating system: Microsoft's development of the *de facto* market standard operating system for PCs confers an advantage to it in the development of application software, exploiting Windows' capabilities to the maximum extent.

For so-called defined standards, the processes of definition and further development of the standard are also important. They can either be open, as in the case of Internet standard-setting processes, or closed, as in the case of many industry or government-dominated standards-setting bodies, in which participation is rigidly controlled, partly to avoid dominance by any one market player or country.

The tensions between open and closed processes, and between *de facto* and defined standards, continue to affect the evolution of ICT in all its manifestations. In networking areas, the dominance of the Internet has led, at least for now, to an emphasis on open processes, which is generally good for the consumer.

Of course, the desire to establish competitive advantage in the market inevitably leads vendors to try to establish proprietary niches for their products within the otherwise open, standards-based environment. After all, there has to be something unique about competing products for them to be worth buying, and it would be natural for companies to hope that the unique features of their products, over time, could lead to the adoption of their approach as a *de facto* industry standard.

Perhaps one of the best examples of a standards war being fought today concerns the browsers offered by Netscape and Microsoft. The technology and architecture of both browsers are open, although there is no guarantee that they will remain so. As part of each upgrade, new features are published openly in a bid to gain dominant acceptance among software developers and web page designers. The stakes in this particular battle are very high.

Relative to a proprietary computing or networking environment, in which all functions have been designed by the vendor with the maximum interoperability in mind, there can sometimes appear to be loss of functionality in moving to an open, standards-based environment. Often, products that claim to adhere to standards do not always

function as integrated units when they come from different companies. *Caveat emptor* was never more appropriate than in the selection of supposedly interoperable software and hardware.

As the security found on the Internet improves with the widespread adoption of standards-based encryption, probably based on PKI, attention will naturally shift to application-layer security issues. The ability for each application to control access to particular records based on the requester, the legislation, guidelines and codes of the particular jurisdiction, and perhaps the unique concerns of the owner of the data, will become paramount. Again, the development of ways of addressing this need based on common approaches and standards will be the only way in which the security features adopted in different jurisdictions or for different applications will be able to operate together.

Education, Communication and Consultation

Instilling public trust and confidence in health information networks will require a broad-based effort to educate, communicate and consult. Such a process must involve all stakeholders, for no one group can be regarded as having all the answers. Policy makers need to better understand the contribution that ICT can make to health; industry needs to better understand the ethical nuances of the health sector; and care providers need to better understand the public's legitimate concerns. While there are few experts on all the issues, each group has something to contribute.

Any efforts at education, therefore, must include all the stakeholders in the system — professional associations, privacy commissioners, universities, federal and provincial health ministries, the private sector and, most importantly, the general public. The interests of these groups may be in conflict in certain areas, but at all levels there is a need for both dialogue and education.

The focus of this multilevel dialogue should be on privacy and confidentiality in the health system, including the weaknesses of the current system, the threats poised by health information networks and how both the threats and the current weaknesses may be addressed by using technology in appropriate ways. Understanding the benefits derived from health networks is as important as understanding how legitimate concerns can be protected in an increasingly networked world.

The federal minister of health should take a leadership role in the development and implementation of a proactive communications strategy in this area, along with provincial counterparts and other opinion leaders. Professional bodies should also be enlisted, as individual health providers will be the key messengers for the benefits of health information networks. They are the ones that patients see, know and trust.

While the overall message of this strategy should emphasize the positive, a balanced approach is also important. Part of the message should be that there is simply no perfectly secure environment in which all personal data are perfectly protected — not today and not tomorrow. As always, security is a matter of degree and protecting data against inappropriate use is inherently a matter of making tradeoffs.

Conclusions and Next Steps

A broad consensus emerged among the participants in the St. John's workshop, focussing on five main points:

First, and perhaps most importantly, there is a need for a proactive communications and consultation strategy that should engage the public, involve both federal and provincial health ministries, and include opinion leaders from the health sector and other key stakeholders.

Second, stakeholders must build an infrastructure for the security of health networks that meets international standards. To this end, public-key encryption and the development of infrastructure for it should be explored. Ensuring that open standards continue to prevail in security, as in other areas having to do with networking, is of fundamental importance.

Third, at the federal level, policy frameworks and principles are required to guide provincial legislation. Such frameworks should build on the CSA Model Code, OECD guidelines and the experiences of other jurisdictions such as Europe.

Fourth, the entire debate in this area will be aided by a consensus on key definitions, including definitions of such concepts as "need to know," "control," "access" and "ownership."

Finally, there is an important role for independent audit and accreditation, or for the identification of a "trusted third party" that would have oversight and compliance responsibilities.

A number of workshop participants are members of Health Canada's newly created Advisory Council on Health Infostructure (ACHI). The ACHI provides an opportunity, over the next year, to further develop an agenda for action relating to privacy, confidentiality and security issues. It would be most helpful if ACHI could be supportive of the type of collaborative and inclusive process described above. One opportunity for ACHI to set out the issues for broader discussion and consultation was at the National Congress on Canada's Health Information Infrastructure in February 1998, which was jointly sponsored by Health Canada and the Government of Alberta.

The knowledge and expertise brought to the St. John's workshop by the participants reflected the wealth of thought and effort that has already gone into addressing the issues of privacy, especially data protection, confidentiality and security across the country. If the workshop was able to contribute anything to the evolving debate on these issues, perhaps it was improving awareness of the benefits of sharing information, knowledge and experiences. Telehealth is an area in which Canada can become a world leader. This will only occur, however, if stakeholders remain dedicated to working together on what are, so clearly, shared problems and concerns. It must be remembered, however, that in this era of continual change — political, social and demographic as well as technological — in all likelihood some further developments are just around the corner that could change everything yet again. In such an environment, collaboration is more than just a valuable thing to do... it may be a matter of survival.

Appendix: Workshop Participants

Speakers

Joan Marie Aylward, Newfoundland Health
Bob Cavanagh, Ontario Health
Elizabeth Davis, Healthcare Corporation of St. John's
Bill Dziadyk, Department of National Defence
André Lacroix, University of Montreal
Bob Little, Entrust/Little Consulting
Denis Morency, Motus Technologies
Andrea Neill, Department of Justice Canada
Linda Weaver, TecKnowledge

Break-out Group Chairs

Andrew Bjerring, CANARIE
Marie Fortier, Health Canada
Bill Trott, B.C. Privacy Office
Mo Watanabe, Professor Emeritus of Medicine

Rapporteurs

Danielle Bertrand, Stentor
Cheryl Doiron, Atlantic Health Sciences Corporation
Ross Fraser, Ontario Health
Mary Marshall, Cook Duke Cox
Doreen Neville, Memorial University of Newfoundland
Tom Noseworthy, University of Alberta

Notetakers

Valerie Gideon, Industry Canada
Marc Lee, Industry Canada
Penny Stratas, Industry Canada
Charlotte Ward, Industry Canada

Participants

Jack Botsford, Operation Online
Alexa Brewer, Health Canada
Janice Cooper, Memorial University of Newfoundland
Rick Domokos, Industry Canada
Rod Elford, Memorial University of Newfoundland
Gerard Farrell, Newfoundland Cancer Treatment & Research Foundation
Ross Fraser, Ontario Health
Daryl Genge, Operation Online
Valerie Hagerman, New Brunswick Health
David Hoye, Industry Canada
Penny Jennett, University of Calgary
Bob Kapitany, Health Canada
Nuala Kenny, Dalhousie University
Erin Keough, OLIN-MUN
Rafiq Khan, CANARIE
David King, Seabright Corp.
Jerry Lee, Health Canada
Pierre Levasseur, Health Canada
Michael Martineau, Software Kinetics
Heather McLaren, Manitoba Health
Elaine Menard, Department of Justice Canada
Paul Mitten, Compusult Ltd.
Masako Miyazaki, University of Alberta
Pierrot Peladeau, University of Montreal
Jocelyne Picot, Industry Canada
Mike Pluscauskas, CHII
Malcolm Rigby, Systems Xcellence
Carl Robbins, MUN/TETRA
Steve Rosinski, TimeStep
Ross Smith, Health Canada
Dorothy Spence, TecKnowledge
Blair Stewart, New Zealand
Robyn Tamblyn, McGill University
Theresa Marie Underhill, Health Canada
Alex Wells, Datadisk
John Williams, SmartHealth
Don Willison, McMaster University
Jennifer Zelmer, CIHI

CANARIE Health Advisory Working Group

Céleste Burnie, CANARIE
Carol Ann Furlong, Industry Canada
Rafiq Khan, CANARIE
Marc Lee, Industry Canada
Pierre Levasseur, Health Canada
Marie-France Rémy, Industry Canada
Penny Stratas, Industry Canada
Mo Watanabe, Professor Emeritus of Medicine

Prepared by

Marc Lee, Industry Canada

Editorial Committee

Andrew Bjerring, CANARIE Inc.
Rafiq Khan, CANARIE Inc.
Mo Watanabe, Professor Emeritus of Medicine