

PRIVACY AND HEALTH INFORMATION: CHALLENGES FOR NURSES AND FOR THE NURSING PROFESSION

"In recent years, privacy has become a matter of increasing concern and debate in health care. This has been spurred by the proliferation of computerized health information systems, electronic health records, databases and registries and by growth in information intensive areas such as genetics.... How should nurses, individually and collectively, address these issues?"

- The sister of a patient in intensive care has approached a nurse for information about the patient's condition. The patient had not previously indicated that he had a sister. Should the nurse provide this information?
- A nurse working in the community wants to study the correlation between average income level (as inferred from publicly available information based on knowing postal codes) and use of health services in the community. Is individual consent required for this observational research?
- A regional health authority contracts a nurse specializing in informatics to assist in developing policy guidelines for a new health information system. The plan calls for the extensive collection of clinical information for purposes of quality assurance, resource planning and accountability. The nurse advises that consent should be obtained for these purposes but is told that it is impractical.
- A hospital is implementing a new health information system based on role-based access. One of the nurses involved on the team argues that the system should provide patients the option of restricting the flow of information and that certain information should be segregated in electronic lockboxes.
- A nurse provides support in the community for a family with a disabled child. The parents want to have another child and are considering genetic testing. However, the father is concerned that the information from his test could also reveal genetic information about his siblings and asks the nurse whether he should seek their approval before undergoing the test.
- The elders in a first nations community seek advice from a nurse who has worked with the community for several years. People are concerned about a new consent form for non-insured health benefits that authorizes extensive sharing of their health information outside the community. And they are upset that if they don't sign the form they will have to pay prescription drugs and other benefits out of their pockets. Although the form is not related to the professional service the nurse provides, they have brought the issue to her because they trust and respect her. She finds the form confusing and indeed is unable to figure out exactly what information sharing it authorizes, or to whom.
- Visiting the home of a new mother, a nurse observes that the baby is distressed. The father and the mother smoke around the baby and the apartment is infested with cockroaches. The diaper has not been changed for some time, contributing to a bad rash – the probable cause



**CANADIAN
NURSES
ASSOCIATION**

**ASSOCIATION
DES INFIRMIÈRES
ET INFIRMIERS
DU CANADA**

of the baby's distress. When these issues are raised with the parents, they admonish the nurse not to meddle in their private life. The nurse believes the baby is at risk.

- A nurse learns that her regulatory body provides registration information, such as information about her position, employer and education to the Canadian Institute for Health Information (CIHI), who use and share this information for research and statistical purposes. She supports the use of information for research and understands that there are in some jurisdictions privacy laws and guidelines for release of information. However, she wonders whether she can control what information is sent.

INTRODUCTION

Privacy is a core value deeply rooted in the nursing profession's history and traditions. Respect for privacy is fundamental in respecting people, their dignity and their autonomy. It is also central to trust in a professional relationship. Patients need to feel free to disclose information to nurses and other health professionals. Without trust, they may withhold or falsify information important to their care.

CONTENTS

Introduction.	2
Definitions.	3
Principles of the Canadian Standards Association's Model Code for the Protection of Personal Information	3
Landmarks and Key Principles in Public Policy Concerning Data Protection	4
The Centrality of Consent in Privacy Debates	5
Select Key Issues.	6
Health Provider Information.	8
Privacy Enhancing Technologies	9
Transparency, Openness and Accountability.	10
Privacy Impact Assessments.	10
Nursing and Public Policy Concerning Privacy.	11
From the CNA Code: Confidentiality	11

In recent years, privacy has become a matter of increasing concern and debate in health care. This has been spurred by the proliferation of computerized health information systems, electronic health records, databases and registries and by growth in information intensive areas such as genetics. Information flows have become increasingly complex, and the demands for health information for a variety of purposes and by a variety of users have increased.

Growth in nursing informatics attests to the professions' willingness and even enthusiasm to use health information and information technology to promote better health and health care. However, as information technologies and databases proliferate, it becomes increasingly challenging to protect this information and for patients to control, or even know about, what happens to their health information.

How should nurses, individually and collectively, address these issues? What is at stake for nurses, patients and the public? In an increasingly interconnected web of health information, what can the public expect from nurses concerning their role in safeguarding privacy? What can nurses accurately and responsibly promise concerning confidentiality? What should they be able to promise?

The vignettes above are intended to indicate a broad range of privacy issues that may arise for nurses. Some are immediate practice issues for which relevant policy principles are more or less settled, although uncertainty remains about the interpretation and application of those principles. Other vignettes touch on matters of broader public policy. These policy issues are less settled, and there is need for public education and greater public dialogue and debate about them.

The Canadian Nurses Association (CNA) has stated the overarching issue straightforwardly in its position statement on *Privacy of Health Information* (2001): "CNA believes individuals have the right to privacy with respect to their personal health information. However, CNA recognizes health information is necessary to improve population health status and to improve the effectiveness and efficiency of the health system" (p. 1). Having clarified the conflicting goods or obligations, the position statement goes on to give greater weight to the right of privacy by adding that "an individual's right to privacy of personal health information is paramount" (p. 1).

CNA's *Code of Ethics for Registered Nurses* is an important starting point for reflection toward resolution of both sorts of issues. However, the broader policy issues are not only for the profession but also for society to resolve in the context of informed public dialogue and debate. These broader

policy issues are the primary focus of this paper. Its main objectives are as follows:

- to promote informed public dialogue and debate about privacy issues;
- to help nurses better understand the policy context in which privacy issues are being debated today, and thereby promoting the informed participation of the profession – both individually and collectively – in discussing and resolving these issues;
- to help nurses become more sensitized to, and able to address, privacy issues that may arise in their practice and relationships with patients;
- to help nurses advocate for their patients and educate their patients about privacy matters, their rights in connection with privacy and the limitations of those rights.

DEFINITIONS

It is important to specify what we mean by privacy and to distinguish it from related notions with which it may be confused. The following definitions are a useful starting point for reflection and discussion:

- **Privacy:** the right or interest in controlling or limiting the access of others to oneself.
- **Informational Privacy:** the right or interest in controlling or limiting the access of others to, and the purposes for which others may use or disclose information about, oneself.
- **Confidential Information:** information that is subject to and protected under a duty of confidentiality, which information may be more or less sensitive, revealing of, or potentially harmful to, the person it is about.
- **Confidentiality:** the duty of someone who has received confidential information in trust to protect that information and disclose it to others only in accordance with permissions, rules or laws authorizing its disclosure.
- **Professional Confidentiality:** the duty of professionals to hold secret that which is revealed to them in the trust of the professional relationship, subject to certain narrowly defined exceptions.
- **Security:** safeguards to ensure that information is processed (accessed, used, disclosed) only as authorized and to prevent unauthorized processing of health information.

PRINCIPLES OF THE CANADIAN STANDARDS ASSOCIATION'S MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION

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 where 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 is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.

Accuracy

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

Safeguards

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

Openness

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

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.

Source: Canadian Standards Association, 1996, Toronto: Author.

- **Provider Information:** information about health providers pertaining to their role in the provision of health care, including registration information and information related to their work activity.

These definitions have two main limitations. First, in their simplicity, they are little more than sketches or outlines – a starting point for reflection and discussion and not a resting place. Second, they are to varying degrees contentious, debatable or subject to different interpretations.

LANDMARKS AND KEY PRINCIPLES IN PUBLIC POLICY CONCERNING DATA PROTECTION

Public policy concerning informational privacy has been shaped by what are called ‘fair information practices.’ Key monuments in the development and evolution of these practices are outlined below in chronological order.

1973: The U.S. Department of Health, Education and Welfare issues its *Code of Fair Information Practices*.

1980: The Organization for Economic Cooperation and Development (Europe) issues *Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data*. These data protection principles influence policy development in Europe and throughout the world.

1986: The Canadian Standards Association (CSA) issues its *Model Code for the Protection of Personal Information*, which lists 10 fair information principles that significantly influence policy development in Canada and elsewhere.

1995: The European Union issues Directive 95/46/EC *On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data*, which not only binds member countries but requires other countries to have protections consistent with its principles as a condition of receiving data from member countries.

2000: Canada issues the *Personal Information and Protection of Electronic Documents Act* (PIPEDA), which incorporates the principles of the CSA Code and meets the requirements of the European Union Directive. It also binds the provinces and territories unless they introduce substantially similar privacy legislation.

2003: On 14 April 2003, the United States passed federal privacy standards (*Health Insurance Portability and Accountability Act of 1996*) to protect patients’ medical records and other health information provided to health plans, hospitals and health care providers.

The statement of principles in the CSA Code and their incorporation into PIPEDA is the culmination to date of an evolving process. It is widely regarded as a state of the art expression of data protection principles.

These principles help to frame the issues and guide the development of policy and practice by signalling relevant considerations. However, they are too general to resolve many of the most important issues. For example, to say that consent is required “except where inappropriate” does not tell us when it is “inappropriate,” which is one of the most hotly contested policy issues today.

In addition, these principles were not specifically developed to deal with health information. For example, the individual access principle as stated does not give recognition to practices within health care whereby patients may be denied access to their own records. Further, the principles are aimed primarily at individuals and do not easily address concerns families or communities may have about shared health information.

The 1999 report of the National Advisory Council on Health Information *Paths to Better Health* was another influential, landmark document. It recommended that the provinces and territories harmonize their laws concerning health information to a common, high privacy standard. PIPEDA has given further impetus to this harmonization. Some provinces have already enacted umbrella legislation specifically covering health information; others are working on it. In addition to changes in statutory law, there are ongoing developments in the common law, including cases that test the *Charter of Rights and Freedom* in connection with health information.

Other policy developments concerning health information in Canada would also include:

- guidelines and codes by various organizations, including professional organizations (e.g., the Canadian Medical Association’s *Health Information Privacy Code*; International Council of Nurses, *Health Information: Protecting Patient Rights*);
- statements and edicts by regulatory bodies clarifying responsibilities in light of the changing legislative landscape;
- sectoral discussion papers and guidelines, such as apply to research using health information (e.g., various documents by the Canadian Institutes for Health Research [CIHR], CNA’s *Ethical Research Guidelines for Registered Nurses*); and

- institutional policies, such as those applying in hospitals, health research organizations, health databases and disease registries.

CNA, like other professional associations and stakeholders in the health sector, has been monitoring and providing input into these policy developments. The future of nursing, and more broadly the Canadian health system, will be shaped in large measure by technological and policy developments concerning health information. It is important that nurses from all walks of the profession, as professionals and advocates for their patients, bring their perspectives, knowledge and experience to bear upon ongoing policy issues.

THE CENTRALITY OF CONSENT IN PRIVACY DEBATES

In the main, privacy issues concerning health information come down to the tension between the need or desire for information sharing, on the one hand, and the right or interest in limiting information sharing, on the other. There are important values on either side of the debate.

Many of these issues, and by far the most difficult and contested ones, have to do with consent. Consent issues divide into two main categories: i) under what circumstances can information be collected, used or disclosed without consent? and ii) where consent is required, what constitutes an appropriate or adequate consent? In addition, safeguards and protections for health information are also important and may have some bearing on what form consent should take or even whether consent is required at all.

Collection, Use Or Disclosure Without Consent

Few would dispute that there are at least some exceptions to the rule of consent. However, what those exceptions are and how broad they should be is a matter of debate. Issues concerning exceptions to the rule of consent link closely to exceptions to the rule of confidentiality. Under what circumstances is it justifiable for a health professional to disclose confidential information without the permission of the person the information is about?

The health professions have been vigilant about keeping exceptions to the rule of confidentiality very strict. Disclosure without consent has been limited to narrowly defined purposes or situations: emergencies, avoiding or preventing a serious and imminent harm to a third party, public health and safety, the administration of justice

and oversight of the profession by a regulatory body. CNA's Code of Ethics is typical in limiting consent exceptions to situations where there "is substantial risk of serious harm to the person or to other persons or a legal obligation to disclose" (CNA, 2002, p. 14). This statement would be an appropriate starting point for the analysis of the vignette above concerning the new baby thought to be at risk.

Even with respect to these relatively narrow exceptions, there has been considerable debate within the health professions. In recent years, pressure has grown to broaden these exceptions. Research, quality assurance, fraud detection and population health are among contested purposes, it is claimed by various persons and parties, that are sufficiently compelling to justify the disclosure of confidential information without consent. The vignette about the regional health authority developing a new health information system illustrates how these systems can facilitate the sharing of patient information for a variety of secondary purposes not directly related to the provision of care. The issue of consent the nurse raises here is an important one. There may be reason to question whether, as the nurse is told, consent is indeed impractical. However, even if or to the extent it is impractical, the mere fact of impracticality is not sufficient to justify the non-consensual information sharing, which would need to be argued on a purpose by purpose basis.

Standards for Appropriate Or Valid Consent

The standards for consent as they have evolved for consent to treatment are higher and more stringent in health care than in other contexts: the consent must be adequately informed and the consent must be voluntary. By contrast, both the CSA Code and PIPEDA, which are primarily oriented to commercial exchanges, speak only of consent and not of informed consent. They also permit negative consents, which places the burden on the individual consumer to "opt out" of an information sharing practice. In effect, the failure of the consumer to opt out is taken as evidence of consent. This is clearly not informed consent as the doctrine has been developed in the health care context. However, some argue that consent may be legitimately implied when patients are notified that their information will be shared with others and, thus informed, fail to opt out.

A number of specific issues are in debate. Are blanket or open-ended consents acceptable in some circumstances? How informed does consent need to be? Who should do the informing? Under what circumstances is

notification, with or without the choice of opting out, acceptable in place of consent? Under what circumstances may consent be implied? The nurse in the vignette who is asked for information about a patient by the patient's sister may believe that the patient's consent to share this information with the sister is implied. However, the patient has not given any indication to support such an inference, and in situations of uncertainty the best policy is to check with the patient.

Yet other issues arise with respect to voluntary consent. Consent can be coerced in a variety of ways, such as requiring someone to agree to certain information sharing as a condition of receiving a needed service. A scenario like this may prompt the elders to ask the nurse for advice. Nurses can play a very important role helping patients who are confused or worried about consent. However, consent can sometimes be of questionable or debatable validity, and in such cases, there may be no straightforward answers to a patient's questions or concerns.

Consent and Appropriate Safeguards

As important as consent is in connection with privacy, there are other considerations, including the existence of adequate safeguards to protect identities and cultural groups, to reduce the risk of harm and to offer provisions in order to ensure transparency and accountability. Indeed, a case can be made that consent requirements or standards can be relaxed if the person cannot be readily identified from the information in question or if safeguards exist to ensure that those in question will not be harmed as a consequence of disclosing their information. Whether or to what extent such safeguards reduce the requirement for consent is a matter of debate; however, it is generally agreed that it is important for such safeguards to be in place regardless of the rules for consent that are in place.

Important values are at stake on either side of these debates. Privacy, autonomy and confidentiality are certainly important values for health professionals. However, health professionals also have obligations to disclose information when third parties are at serious risk, as well as commitments to improve the health system and the overall health of the population. These obligations and commitments are also of great importance.

SELECT KEY ISSUES

In what follows, a few select issues are described. One's position on these issues will depend on which among competing values are given greater weight or importance.

Research

The capacity of health professionals to achieve the ends of their profession – whether through the provision of services to those who are sick or measures to keep people healthy or improve health – depends upon knowledge. Thus, the advancement of knowledge has been a central value in the health professions. However, throughout history the acquisition of knowledge has proceeded in a more or less unsystematic way. Today, there is increased emphasis on the evidence and research necessary to acquire and test knowledge that health professionals use in their practice. Notwithstanding certain reservations and qualifications, the health professions have embraced research in the name of enhancing professional practice and enhancing health. Increasingly, research methods and tools are being integrated into the nursing curriculum and the ethic of research is being promoted.

The challenge is that research may be more or less privacy invasive. Research in population health and the broader determinants of health heightens these issues, because it often relies upon the collection of vast amounts of information concerning sensitive matters such as lifestyle, financial situation and personal relationships. In some instances there is a conflict between the goals of research and privacy. Issues may arise not only for nurses conducting or directly involved in research but also for nurses who interact with researchers or whose patients are research subjects. As advocates for their patients, nurses also advocate on behalf of their patient's privacy. How should conflicts between privacy and research be resolved? When, if ever, is research without consent justifiable? What should the nurse do if he or she believes that certain research is ethically unacceptable?

The issues raised by the vignette about the nurse researcher will become more and more prominent as research takes advantage of electronic health records and databases. Should the nurse researcher be required to obtain the consent of patients to link data about their use of health services with publicly available information? Regardless of this link, should the nurse researcher be able to access information about the use of health services without the permission of patients? Various guidelines exist to assist nurses to work through these and other questions, such as the CNA's *Ethical Research Guidelines for Registered Nurses* (2002). However, many issues arising in connection with research are unsettled as a matter of public policy and subject to ongoing public debate.

Information Sharing Among the Health Team

The health professions are moving toward an integrated, collaborative approach to the provision of health services. Nursing has strongly advocated such an approach. However, greater integration and collaboration may require greater sharing of information if the various members of the team involved are to contribute safely and effectively. Privacy protections have the potential to impede such information sharing.

CNA's Code of Ethics (2002) advises nurses "to inform the persons in their care that their health information will be shared with the health care team for the purposes of providing care" (p. 14). This advice appears to be based on the assumption that consent is not required for sharing information among members of the health care team. This is a matter of debate in some contexts, such as the mental health field and small communities where people may want at least some of their health information protected from some persons who may be involved in their care. One of the advantages of computerized records is that they can facilitate the patient's choice in restricting aspects of their information from certain providers. However, whether as a matter of policy such choice should be permitted, and under what conditions and limits, is contentious. The nurse in the vignette who argues that the hospital's health information system should have a 'lock-box' feature is on solid ethical ground, but the issue is certainly open to debate. Regardless of how this issue is resolved in policy, it is important to communicate policy concerning this issue both to patients and members of the team, not only out of respect for the patients but also in order to avoid confusion or uncertainty among members of the team.

Protected Information

Health information is especially sensitive and thought to warrant a very high level of protection. However, the question of what constitutes health information and should be thus protected is more complex than it appears to be at first glance, particularly when one considers the broad definitions of health and types of information that may be collected for population health. In addition, one needs also to consider the increased potential for data linkages with various other types of information.

Many policy documents afford protection only to "personal information." Following this approach, when personal information is "deidentified" it is no longer "personal information," and therefore, not deemed worthy of protection. There are several problems with this approach, however. One reason that even so-called "de-

identified" information may warrant protection is that deidentification may be more or less imperfect, and the potential that someone can be identified may be more or less great. In addition, some people may be concerned about how information may stigmatize the group to which they belong, even if individually they cannot be identified. Some may object to their information being used for certain purposes of which they disapprove. Others may feel that if their information has commercial value, they should receive a share of the benefit. Finally, some argue that their right to decide what happens to their personal information includes having some control over its deidentification and subsequent use for whatever purposes.

Commercialization of Health Information

Health information is becoming a more valuable commodity. At the same time, the line between the private, for-profit sector and the public, not-for-profit sector is becoming more and more blurred. Increasingly, research projects are sponsored by or partnered with commercial entities. Indeed, it is becoming more commonplace for granting agencies to reward or require such partnerships, and plans for commercialization, in their adjudication criteria. The development of health information systems also brings in a variety of partnership and financing arrangements, such as those being pursued by Canada Health Infoway. Research in genetics is highly commercialized and has given rise to novel entities like the privately owned Icelandic database, which links large amounts of population data derived from detailed genealogies, health records and DNA samples.

From a privacy standpoint, commercialization gives focus to issues concerning ownership and control of health information and of body parts or tissues that reveal genetic information. As a rule, people are more inclined to share their information for purposes they hold to be of social value. The social value of activities like drug manufacturing, marketing and even hospital fundraising may be questionable or not sufficiently important to justify non-consensual use or disclosure. In addition, there may be greater reason for concern about accountability for information in the private sector than in the public sector.

Mandatory Reporting

Mandatory reporting in certain instances has long been accepted and endorsed by the health professions. However, because it infringes on privacy and professional confidentiality, the justification for mandatory reporting has been stringently limited to preventing

serious harm to third parties, as in the case of communicable diseases or child abuse. Even so, there has been debate within the health professions about how great or how imminent the anticipated harm must be and how certain one must be in one's assessment of risk. In some cases, health professionals may be uncertain about whether to report. In the vignette about the new baby, such risk as there may be does not appear to be either serious or imminent. The diaper rash may indicate neglect but that is not the same as abuse. However, although the situation does not appear to be one that warrants reporting, there may be nursing interventions, such as education, by means of which to address the issue.

A shift is taking place toward extending mandatory reporting rules to cover a broader range of cases and a broader justification than harm prevention. From a public health perspective, it is useful to have surveillance information not only about communicable diseases but also about a variety of disease and health conditions. The information needs of population health are virtually limitless, and the warrant for collecting such information extends beyond harm prevention. What principles should govern the reporting of health information to various authorities? Should this be limited to harm prevention or is it appropriate to extend it to the promotion of health or to other purposes such as monitoring the health of the population in order to better allocate resources? In deliberating about such issues, it must also be considered that, in addition to its adverse impact on patient autonomy, mandatory reporting can also diminish the trust patients place in health professionals. Ironically, mandatory reporting can create its own harms if members of vulnerable or stigmatized groups withhold information or avoid seeking care due to fears about lack of confidentiality.

Group Privacy and Community Consultation

Although privacy primarily concerns individuals, it also has application for families, groups and communities. In the case of genetics, for example, information about one sibling can be very revealing about other siblings or about the family. To this extent, one can argue that the information is about or belongs to the family or even the community, not only the individual member. Others besides the person from whom genetic information is extracted may share a privacy or an access interest in the information thus revealed. This greatly complicates the issue of consent, as evident in the vignette involving the patient who asks the nurse whether he

should get approval from his siblings before undergoing a genetic test that will indirectly reveal information about them. There may be no right or wrong answer to this question, but the nurse can at least help the man think through the issue.

The general issue is by no means limited to genetic information or to family situations. Members of a community may have an interest in keeping things private with respect to various outsiders, including researchers, as well as an interest in how they may be represented or misrepresented as a group. Persons with HIV may be concerned about how information extracted from their group may be used contrary to their interests or values. Aboriginal people may be concerned that information gleaned from their community – even if accurate – may be used to perpetuate stereotypes that are hurtful to the community. They may also be concerned as a matter of principle having to do with rights of ownership, control, self-determination or self-governance with respect to their information. It may be these sorts of concerns that are raised by the consent form in the earlier discussed vignette concerning the first nations community.

Along these lines, some commentators have advanced the concept of “group privacy” to express an interest in privacy that is shared among a group and that is not reducible to the interests of its individual members. The idea of community consultation, whereby communities collectively have some control over the collection of information about them, has been proposed partly in response to group privacy. However, it raises challenging issues having to do with consent and representation that are the subject of ongoing debate.

These are but a few of the key issue areas in public policy today around which debate is occurring. They are unlikely to be settled in the near future. Nurses can make a significant contribution by being involved in the research, dialogue, public debate and policy work surrounding these issues.

HEALTH PROVIDER INFORMATION

Similar factors as have heightened privacy issues in connection with patients also come into play with health providers. Provider information could include a range of things, ranging from registration information to information correlating someone's practice interventions with various health outcomes.

Provider information is increasingly sought by a variety of people and organizations for a variety of purposes.

Foremost among these, regulatory bodies require certain information in order to discharge their mandate. Measures to monitor errors and mishaps and to improve practices and systems for the safety and well being of patients may likewise require provider information.

These purposes have been accepted, and indeed promoted, by the health professions as a matter of professional accountability, notwithstanding ongoing debates about precisely how the principle is implemented (e.g., precisely what information is collected, subject to what controls, etc.). However, other purposes, even important ones, are less compelling. For example, the nursing profession recognizes the importance of research on a range of topics, including the relationship between nursing interventions and health outcomes and human resource issues in nursing. Indeed, nurses are very active in such research and hopeful that this research will lead to both improved quality of work life for nurses and improved care. Are such purposes compelling enough to justify the collection, use or disclosure of provider information without consent?

Regulatory authorities forward provider information to CIHI. This includes sex, year of birth, year of graduation, education, employment status, place of work (e.g., hospital, educational institution), primary area of responsibility (e.g., ER, oncology, teaching, research), position (e.g., chief nurse officer, staff nurse, researcher) and postal code. Some nurses may question the right of the regulator to collect all of this information, notwithstanding the legitimacy of the purpose and that there are letters of agreement between the regulatory bodies and CIHI. Many regulatory bodies inform their members on annual renewal license forms that data is released for research purposes. What controls should be in place to protect whatever data is collected? Is it sufficient for an organization to determine what information is released based on its own institutional policy or should the nurse be notified directly?

In its position statement *Collecting Data to Reflect the Impact of Nursing Practice* (2001), CNA proclaims “data involving identifiable health information should only be used with the consent of the individual” (p. 1). This is surely intended as applying to the patient, but does or should it also apply to health providers? Some argue that information about providers is not “personal information” but rather “professional” or “workforce” information, and therefore, exempt from requirements for the protection of personal information. Certainly there is greater reason for protecting patient’s health information. However, it does not signify that provider information is not personal information or that it also does not warrant protection.

Issues with respect to provider information are likely to intensify in light of rising desire, need or demand for this information. If these issues have not been prominent to date, the reason probably has more to do with the fact that providers are generally unaware of the extent that information about them may be collected, used and disclosed without their consent, rather than the importance of the issues. The nurse in the vignette dealing with provider information may object for any number of reasons to the release of her information without her consent. Even if these reasons can be countered by compelling argument, it can be argued that this information sharing should be justified and more broadly publicized to nurses. It is important for nurses to contribute and be involved in research and discussion that will illuminate and help resolve these issues.

PRIVACY ENHANCING TECHNOLOGIES

Information technology is often associated with increased threats to privacy. Older information systems, with pieces of paper dispersed in various “silos,” may have been less efficient but made it more difficult for third parties to access information. Certainly with the capacity for increased information reproduction, flow and centralization, the potential is there for increased loss of privacy. However, the problem lies less with technology itself rather than with the rules under which we operate this technology. And just as technology affords the potential for increased loss of privacy, it also affords opportunities to enhance privacy as well. A selection of important initiatives in the area of what are called “privacy enhancing technologies” is outlined below.

- **Deidentification:** An important privacy protection principle is that information should be in the least intrusive form possible. Deidentified information is thus preferable to identifiable information and the more perfect the controls to prevent reidentification the better. Moreover, many of the purposes for which health information is collected, used or disclosed can be achieved with little or no compromise using information that has been deidentified to some degree or other. The removal of identifiers is the most obvious way of achieving this, but others are being experimented with, including the introduction of ‘noise’ into databases that confound reidentification. To the extent that technology can help prevent reidentification, it may help enhance privacy.
- **Encryption:** Encryption involves scrambling information so that only persons privy to a special key are able to open it. By controlling access to these keys, it is possible to

store and transfer information without worrying about it being intercepted or seen by unauthorized persons. This technology is particularly useful for communication over the Internet, because even if someone intercepts an e-mail or hacks into a web site in which personal information is stored, they are unable to read the information without the required key.

- **Audit Trails:** Audit trails digitally record each time a particular piece of information is accessed, indicate who accessed it, at what time and so forth. When people are aware that their behaviour may be subject to monitoring, they are more likely to be careful about what they access and why. Audit trails thus discourage inappropriate access to information and promote increased accountability.
- **Electronic Consents:** One of the main concerns about consent is that the processes for facilitating and recording consent can be burdensome, particularly in cases where the consent allows for different pieces of information to be treated differently. In electronic environments such burdens can be greatly lessened. For example in the paper world, it is cumbersome to sever parts of a record so that members of the health team have access to only the part necessary for them to perform their respective roles and not to items the patient may wish to restrict more narrowly, such as an abortion or episodes involving mental illness. In electronic environments, it is possible to mark off different fields in a database and even create electronic lock-boxes to allow differential access to information depending on considerations such as need to know or patient consent.
- **Layered and Role-Based Access:** One of the challenges of information systems is to ensure that the right people get the right information at the right time. This is especially important in health care. In the paper world, achieving this can be very difficult. In electronic environments the flow of information to the right persons can be facilitated, and the information protected, with passwords and access codes.

Nursing has been proactive in the area of health informatics and is in a good position to ensure that information systems are developed in ways that facilitate the flow of information as necessary for the provision of care, including the protection and even promotion of privacy. However, it is important to realize that the overarching issues are not technological ones but policy or ethical issues. They have to do with the fundamental principles that should constrain the development and implementa-

tion of technology, and in particular, the rules governing access to information.

TRANSPARENCY, OPENNESS AND ACCOUNTABILITY

Measures to promote transparency, openness and accountability are important features of contemporary thinking about privacy and data protection. Audit trails illustrate the logic of the connection. When people know that their behaviour in connection with private or confidential information is subject to scrutiny they are more likely to be sensitive to and respectful of other people's privacy.

Privacy and data protection rules and legislation tend therefore to include provisions requiring those who hold information to establish policies describing such things as the purposes for which they collect, use and disclose information. They also provide an avenue for individuals to gain access to information about them that is held. There is also a requirement to inform patients about these policies. This helps enable individuals to achieve control with respect to their information – awareness being a condition of being able to exercise control. The basic message to those who hold data is fairly simple: centrally record practices and policies concerning health information and ensure they are made available to patients in the system so they know the rules of the game.

PRIVACY IMPACT ASSESSMENTS

Privacy impact assessments have emerged as an important component of privacy and data protection and, in some contexts, are mandated in legislation. They will become increasingly common in health care contexts, and it is important, therefore, for nurses to understand what they are and what they are supposed to accomplish.

Privacy impact assessments sensitize system developers to privacy concerns and flag potential privacy issues, thereby helping to ensure that privacy considerations are incorporated from the outset. They also help to promote increased openness, transparency and accountability, particularly when the assessment is publicized or released for public discussion.

Standards with respect to privacy impact assessments are emerging. Many assessments are little more than checks for compliance with legislation whereas others reach further to try to assess the actual impact on privacy, perhaps going so far as to invite representatives from the patient group to

provide input. The precise elements that go into a privacy impact assessment may include descriptions with respect to the following:

- the information or types of information collected;
- the purposes for which it may be collected, used or subsequently disclosed;
- individuals or organizations, or classes of the same, who may access the information and under what circumstances;
- the use of privacy enhancing technologies where feasible;
- security safeguards;
- provisions for training staff in policies and procedures;
- the legislative authority under which the system operates;
- the rules under which the system will operate, including rules concerning consent;
- impact on professional relationships and on the trust of those relationships;
- impact on the willingness of patients to disclose information; and
- justification for provisions concerning consent, particularly in cases where consent may be bypassed.

Given the complexity of information flows in today's health institutions and systems, gathering much of this information can be challenging for organizations. However, it is necessary if an organization is to be accountable. Moreover, where this information is gathered before the system is implemented and rules have become solidified, it can be very valuable for system and policy design.

NURSING AND PUBLIC POLICY CONCERNING PRIVACY

Nurses face a myriad of privacy issues in their daily professional practice. CNA's Code of Ethics provides useful advice for dealing with these issues. However, some of the issues discussed here are broader issues of public policy that will not be resolved for some time. CNA's Code of Ethics enjoins nurses to "advocate for and respect policies and safeguards to protect the person's privacy" (p. 14). It is important for nurses to understand that they have a responsibility to protect privacy, obtain informed consent, follow agency policies and question policies that are not reflective of current ethical, practice standards and relevant legislation. It is also important for nurses,

FROM THE CNA CODE: CONFIDENTIALITY

Nurses safeguard information learned in the context of a professional relationship, and ensure it is shared outside the health care team only with the person's informed consent, or as may be legally required, or where the failure to disclose would cause significant harm.

1. Nurses must respect the right of each person to informational privacy, that is, the individual's control over the use, access, disclosure and collection of their information.
2. Nurses must advocate for persons requesting access to their health record subject to legal requirements.
3. Nurses must protect the confidentiality of all information gained in the context of the professional relationship, and practice within relevant laws governing privacy and confidentiality of personal health information.
4. Nurses must intervene if other participants in the health care delivery system fail to maintain their duty of confidentiality.
5. Nurses must disclose a person's health information only as authorized by that person, unless there is substantial risk of serious harm to the person or to other persons or a legal obligation to disclose. Where disclosure is warranted, information provided must be limited to the minimum amount of information necessary to accomplish the purpose for which it has been disclosed. Further the number of people informed must be restricted to the minimum necessary.
6. Nurses should inform the persons in their care that their health information will be shared with the health care team for the purposes of providing care. In some circumstances nurses are legally required to disclose confidential information without consent. When this occurs nurses should attempt to inform individuals about what information will be disclosed, to whom and for what reason(s).
7. When nurses are required to disclose health information about persons, with or without the person's informed consent, they must do so in ways that do not stigmatize individuals, families or communities. They must provide information in a way that minimizes identification as much as possible.
8. Nurses must advocate for and respect policies and safeguards to protect and preserve the person's privacy.

Source: Canadian Nurses Association, 2002,
Code of Ethics for Registered Nurses. Ottawa: Author.

individually and collectively, to add their voices to these policy discussions. Indeed, given the profession's emphasis upon public education and the empowerment of patients and communities, nursing is ideally situated to facilitate and promote public education, dialogue and debate about privacy issues.

Nurses can do a great deal to participate in, and shape, public policy concerning privacy and to ensure adequate respect for privacy in professional practice including:

- further education in privacy issues and the values and concepts by means of which to analyze them;
- further knowledge of law, professional codes and institutional policy concerning privacy, particularly as it applies to one's professional practice;
- further sensitivity to privacy, particularly bearing in mind that much privacy infringement is due not to a values conflict but to inadvertence or carelessness, such as discussing details about a patient on a crowded elevator;
- foster research about privacy issues and their impact on patients, families and communities;
- participate, individually and collectively, in public policy debate and formation;
- participate in the formation and review of institutional policies and practices;
- participate in the design of health information system to ensure that privacy concerns are adequately addressed;
- educate patients, families, and communities about their privacy rights and limitations to those rights.

REFERENCES

- Canadian Medical Association. (1998). *Health information privacy code*. Ottawa: Author
- Canadian Nurses Association. (2001). *Position statement: Collecting data to reflect the impact of nursing practice*. Ottawa: Author.
- Canadian Nurses Association. (2001). *Position statement: Privacy of personal health information*. Ottawa: Author.
- Canadian Nurses Association. (2002). *Code of ethics for registered nurses*. Ottawa: Author.
- Canadian Nurses Association. (2002). *Ethical research guidelines for registered nurses*. Ottawa: Author.
- International Council of Nurses. (2000). *Health information: Protecting patient rights*. Geneva: Author.

Ethics in Practice is published by the Policy Regulation and Research Division of the Canadian Nurses Association (CNA).

Free copies are available to all CNA members. For additional information and/or additional copies contact CNA Publications.

For more information mail, fax or e-mail:

Canadian Nurses Association

50 Driveway

Ottawa ON Canada K2P 1E2

Telephone: 1-800-361-8404

or (613) 237-2133

Fax: (613) 237-3520

E-mail: prr@cna-aicc.ca

Web site: www.cna-aicc.ca

ISSN 1480-9990