

Is There A Case for Health Specific Privacy Legislation In the NWT?

Prepared for:
Department of Health and Social Services
Government of the Northwest Territories

By:
Field Law LLP

July 2007

I. INTRODUCTION

The Case for Health Privacy Legislation

This discussion paper has been identified as an essential step in communicating and consulting with stakeholders prior to making any decisions to take the next steps in the development of privacy legislation specific to health information (a "Health Information Act" or "HIA"). This step towards new legislation has great significance for healthcare administration and delivery. It also has notable importance given the increasing trends to legislate privacy obligations that are transpiring in most other Canadian jurisdictions.

This trend is a function of increased awareness of privacy rights generally, and specifically its interplay with how personal information is managed by the state. Loss of control over the management of information, particularly in today's context of globalization, poses serious risks to public confidence, and consequently a state's ability to effectively govern.

Privacy has long been considered a fundamental right in Canada. The United Nations Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights enshrine privacy as a core human right or value that goes to the very heart of preserving human dignity and autonomy, as does the Canadian Charter of Rights and Freedoms. For most Canadians, privacy is about control - the right to control one's personal information.¹

Technology has increased the ability of governments, businesses and organizations to collect, track, and access information. Several surveys over the past two decades have revealed the disquiet of Canadians about government and private sector intrusions into their privacy. Privacy, one of the hallmarks of a democratic society, is being challenged from many quarters, aided by increasingly intrusive and affordable technologies. Compounding these challenges in some cases is an attitude that privacy must be sacrificed for other social goods – national security and business efficiency prominent among them. Data mining, workplace and public surveillance, SPAM and biometric techniques such as facial recognition and DNA identification are collectively mounting a persistent attack on privacy. The same technologies that facilitate modern commerce can also facilitate identity theft and Internet fraud such as "phishing." Technologies that are harnessed for malevolent reasons can cause profound damage to the individuals whose personal information is misused.² And yet from another perspective, it can be argued that technological advances may help protect privacy. While this may be the case, it can equally be argued that such advances alone will not sufficiently protect

¹ Privacy Matters: The Federal Strategy to Address Concerns About the USA PATRIOT Act and Transborder Data Flows, Treasury Board of Canada Secretariat, online: < http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp03_e.asp >

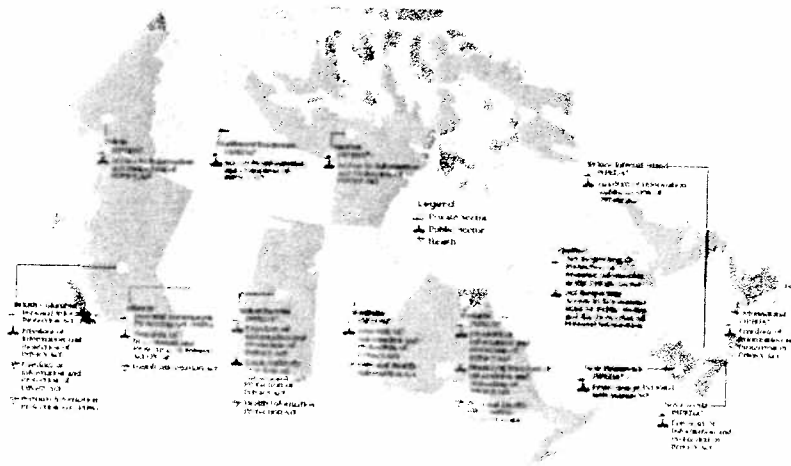
² PIPEDA Review Discussion Document, Protecting Privacy in an Intrusive World (July 2006), online: < http://www.privcom.gc.ca/information/pub/pipeda_review_060718_e.asp >.

Any opinions or views in this paper are those of Field Law LLP and do not necessarily represent the views of the Department of Health and Social Services.

personal information and earn public confidence. In fact, the expeditious manner in which emerging technologies manage and transfer information may constitute a challenge itself.

Correspondingly, public concerns regarding the collection, use, and disclosure of personal information remain, and are likely only increasing. This growing concern has been reflected in surveys conducted to measure public attitudes toward privacy. The Office of the Privacy Commissioner of Canada, in its Annual Report to Parliament 2005, reported that Canadians strongly supported laws protecting their privacy. Additionally, a survey undertaken by the Office of the Privacy Commissioner indicated that 70% of Canadians felt that their privacy had been eroded.³ Accordingly, it is not surprising that all Canadian jurisdictions maintain some form of privacy legislation. Given the above discussion, it is also not surprising that privacy legislation in Canada shares the commonality of incorporating rules that deal with both: i) organizations' obligations regarding the collection, use, and disclosure of personal information; and ii) individuals' rights to access and correct personal information. In essence, these legislative models all support the view that Canadians have the right to know and should feel free to ask why an organization is collecting, using or disclosing their personal information as well as the right to check their personal information and correct any inaccuracies.

There are however some important aspects that differentiate privacy legislation in Canada. Some jurisdictions only maintain legislation with properties similar to the GNWT's Access to Information and Protection of Privacy ("ATIPP") Act⁴ - that governs only the public sector - while other jurisdictions maintain legislation akin to the ATIPP Act as well as other legislation that governs the private sector. As a consequence, and as illustrated below, today's privacy legislation landscape in Canada is layered and complex:



³ Office of the Privacy Commissioner, Annual Report to Parliament 2005, online: <http://www.privcom.gc.ca/information/ar/200506/2005_pipeda_e.asp#toc>.

⁴ S.N.W.T. 1994, c.20.

(See Appendix A for larger image and publishing credit)

Most significant to this discussion paper, note a further differentiation; Alberta, Manitoba, Ontario, and Saskatchewan (the "Health Privacy Provinces") have, in addition to their respective legislation akin to the ATIPP Act, and in some cases also legislation governing the private sector, legislation specific to health information.⁵

The Case for Health Specific Privacy Legislation

The driving force behind the legislation in Health Privacy Provinces can be understood, in part, by looking to the purposive provisions in such pieces of legislation. These provisions refer to the need for strong mechanisms to protect health information,⁶ likely a consequence of the recognition that health information, as opposed to other personal information, is particularly valued by individuals.

In 2000, the Office of the Information and Privacy Commissioner in Alberta completed a benchmark survey of Albertans' attitudes towards privacy, which demonstrated an increasing concern about the use and disclosure of personal information.⁷ When asked to rate the importance of privacy for specific types of information, health records were rated as very important by 80% of the respondents. Only personal financial information received a higher rating. A follow-up survey in 2003 indicated that privacy is increasingly important for Albertans.⁸ This survey also indicated that more Albertans (89%) felt that it was important to keep personal health information safe and private.⁹

⁵ Health Information Act, R.S.A. 2000, c. H-5; Personal Health Information Act, S.M. 1997, c. 51; Personal Health Information Protection Act, 2004, S.O. 2004, c. 3; Health Information Protection Act, S.S. 1999, c. H-0.021.

⁶ See for e.g Alberta's Health Information Act at s.2(a) " ... to establish strong and effective mechanisms to protect the privacy of individuals with respect to their health information and to protect the confidentiality of that information".

⁷ Province of Alberta, Office of the Information and Privacy Commissioner, *Albertans' Awareness of and Views on Privacy Issues*, online: <<http://www.oipc.ab.ca/publications/surveys.cfm>>.

⁸ Province of Alberta, Office of the Information and Privacy Commissioner, *OIPC Stakeholder Survey, 2003, Highlights Report*, online: <<http://www.oipc.ab.ca/publications/surveys.cfm>>. Note: Respondents overwhelmingly agree that it is important to protect individual privacy in Alberta (98% agree), an increase of 10% from the 2000 benchmark survey. Nearly three-quarters (74%) of respondents are concerned that the privacy of personal information is at risk in Alberta, a significant increase from the 56% recorded in the 2000 survey. Eighty-two per cent of respondents are concerned about the privacy of their own personal information, an increase of 11% from the 2000 survey. Eighty-three per cent of Albertans are more concerned about the privacy of their own personal information than they were five years ago, an increase from the 76% recorded in 2000. Sixty-one per cent of respondents strongly agree with the statement, essentially the same level recorded in 2000.

⁹ *Ibid.*

Moreover, in the past twenty years there has been significant judicial development marking the particular value placed on health information. This is in large part a construct of the recognition that the healthcare provider/patient relationship is unique and requires special protection; patients rely heavily upon healthcare providers to keep their health information confidential. This relationship of trust was described as a fiduciary relationship by the Supreme Court in *Norberg v. Wynrib*.¹⁰ The fiduciary relationship between a healthcare provider and patient was then considered in the context of health informatics by the Supreme Court in *MacDonald v. McInerney* which concluded that information disclosed to a physician in the course of treatment "remains, in a fundamental sense, one's own."¹¹ From this line of jurisprudence comes the frequent analysis that a healthcare provider might be the actual owner of the physical or electronic record, but the patient maintains an interest in and general control over the information.

More recently, key stakeholder and interest groups in Canada dedicated considerable efforts to the harmonization of health privacy issues and the management of health information generally. The *Pan-Canadian Health Information Privacy and Confidentiality Framework*¹² (the "Framework") was developed by the Advisory Committee on Information and Emerging Technologies of the Federal/Provincial/Territorial Conference of Deputy Ministers of Health. The Framework is the consequence of extensive consultation and research. Being relatively current (released in 2005), and having the benefit of its findings reflecting consultation in the Health Privacy Provinces, the Framework presents as a tremendously valuable tool to inform and influence any privacy legislative process, including the GNWT's.

In summary, while regulation through legislative measures can serve as an effective means of mitigating against breaches of privacy, such measures must, in attempting to keep pace with emerging technologies, strike a fine balance between flexibility and predictability. It is for this reason that a HIA may benefit the provision and overall success of healthcare in the NWT: a HIA could be tailored to create obligations specific and meaningful to the management of health information.

II. OBJECTIVES

The main objectives of this discussion paper are to communicate on the subject matter and elicit commentary. It is expected that there will be further information to consider and synthesize with respect to gaps in the current legislative scheme and the benefits and challenges of a HIA.

¹⁰ [1992] 2 S.C.R. 226.

¹¹ [1992] 2 S.C.R. 138, 93 D.L.R. (4th) 415.

¹² Online: < http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index_e.html>

The goal behind these objectives is to prepare a more detailed and informed plan for more specific stakeholder consultation. Responding to the questions and learning from the feedback that this paper's audience puts forward will better position interviewers to conduct efficient and meaningful interviews. This in turn is expected to help fulfill the greater goal of drafting meaningful legislation that accurately reflect the needs, beliefs, and practical considerations of stakeholders and, most importantly, NWT residents.

Once initial feedback is received, the time and need, if any, for further education efforts and ongoing discussion will be assessed and will guide the setting of project milestones. In general, the upcoming milestones include:

1. Establish Steering Committee and Work Plan, including consultation plan [end of 2007]
2. Prepare detailed discussion paper(s) [2008]
3. Stakeholder consultation activities [2008]
4. Develop formal legislative proposal [2009]

According to this general schedule, it is unlikely that legislation could be in force earlier than 2011.

III. THE CURRENT STATUS OF PRIVACY PROTECTION FOR HEALTH INFORMATION IN NWT

The current legislative scheme under the *ATIPP Act* may be limiting in its ability to accommodate new modes and approaches of improved healthcare service administration and delivery. The following sets out the main reasons for this assertion.

Collection and Use

Read together, the collection provision under s.40(c)(i) and the use provision under 43(a) of the *ATIPP Act* may pose limitations in how health information can be collected and subsequently used in health systems, particularly with respect to how information can be used for planning and management purposes. This subsection of s.40 requires that

“[no personal information may be collected unless] the information relates directly to and is necessary for (i) an existing program or activity of the public body, or (ii) a proposed program or activity where collection of the information has been authorized by the head with the approval of the Executive Council.”

First, absent clearly established programs or activities for health systems planning and management, it can be argued that health information cannot be collected to fulfill this purpose. Accordingly, a critical review of established programs or activities is required,

including the potential scope afforded under GNWT Policy 49.00: *Health and Social Services Establishment Policy*, particularly section 5(2) that sets out the arguably broad duties of the Minister. In any event, while programs and activities can be created, or clarified, legislation that specifically contemplates the common purposes for which health information is collected may be of benefit. It may also be beneficial to consider the utility of creating collection provisions that, at least in part, are based on a consent model, such as, and for example only, consent to collect information for biobanking purposes. Second, if such programs and activities are not clearly set out, the provisions respecting permissible uses may pose further limitations. Section 43(a) provides that personal information may only be used "for the purpose for which the information was collected or compiled, or for a use consistent with that purpose". Accordingly, the operation of these provisions is to limit secondary uses; and, unless it is argued that planning and management is a purpose that is consistent with the purpose of delivering care (or such other existing program or activity) the case for establishing a HIA to help clarify policy intent is made stronger.

Also, the obligation set out under s.41 of the *ATIPP Act* (to collect, where reasonably possible, directly from individual) may not have sufficient exceptions to adequately accommodate collection of the health information from persons other than the individual. While the current delivery of health services may operate harmoniously with s.41, it may pose a challenge as new modes and methods of information flow are adopted to support the delivery and administration of health services. This may be particularly the case with evolving electronic health record¹³ ("EHR") systems. As EHR systems are introduced, options and reconfigurations can be arranged to more effectively manage information. That is, the existing *ATIPP Act* paradigm, while still affording some flexibility, will not in practice act as an impediment to the introduction of an EHR system. As this system is modified, enhanced, and generally used to its greatest potential however, greater certainty with respect to access/user rights and safeguarding obligations is well merited. It has been noted that an EHR is a mechanism for sharing health information about an individual between multiple sources and must be capable of supporting many different patient/healthcare provider relationships.¹⁴ Further, given the contemplated inter-jurisdictional uses of the GNWT's potential EHR system, the case for, and value of a HIA, is further advanced.

¹³ An EHR is considered a secure and private lifetime record of an individual's key health and care history. An EHR commonly gives authorized health care professionals access to patient's health histories including: a) laboratory and radiology tests; b) hospital visit and discharge summaries; c) physician visit summaries; d) prescribed drugs; and e) immunizations. In contrast, an electronic medical record (EMR) is a clinical information system that describes the record of periodic care provided by one institution. It is a complete patient record, accessible from a single, automated health care provider system. It is a specific internal database related to the particular institutional source. An EMR is sometimes known as an electronic patient record (EPR).

¹⁴ Health Chief Information Officer Council, *Framework for an Electronic Health Record for British Columbians* (British Columbia: January 2003).

Safeguards - Electronic Databases

The provisions of the *ATIPP Act* that impose obligations for safeguards are set out in section 42. This section reads:

The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

An observation can be made that the wording in this section is overly broad and may not specifically address risks specific to the systems that manage or enable the flow of health information. In the pieces of legislation that the Health Privacy Provinces have enacted there is, generally, an obligation on custodians to take reasonable steps to maintain administrative, technical and physical safeguards to protect the confidentiality of information and safeguard access. In some legislation, an obligation is imposed on healthcare providers to take all steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure. Also, if the information is stolen, lost or accessed by an unauthorized person, healthcare providers are obligated to notify the affected individual at the first reasonable opportunity. Such provisions help import an added level of confidence in how health information is managed, particularly when legislation also maintains serious sanctions (such as fines) for breaches.

The case of EHR serves as a good example to support the case for enhanced and more specific safeguarding provisions. It is also a significant and highly relevant example given that the GNWT is embarking on a project to adopt such a system and to have it operate uniquely across Territorial/Provincial borders.

First, it is well argued that EHRs are of significant benefit to the delivery and administration of healthcare:

EHRs allow large amounts of patient information to be gathered, linked and disclosed. EHRs can potentially facilitate the secondary use of patient data and create a large pool of data ideal for use in medical research and health system management. EHRs can be used to link previously unlinked data using unique identities and can allow the accumulation of valuable data, which will create new demands for access. EHRs can be seen as a means to improve care provided to individuals by ensuring that accurate and relevant information is available at the point of care; enhancing quality assurance; allowing for additional health research, and improving public health surveillance.¹⁵

¹⁵ G.G. Griener, "Electronic Health Records and the Protection of Privacy" (2004) 14(2) *Health Ethics Today* 2.

In regards to the drawbacks of using traditional paper records, the Romanow Commission has stated:

Paper records are increasingly becoming obsolete and inadequate. They limit the flow of information, insufficiently document patient care, impede the integration of health care delivery, create barriers to research, and limit the information available for administration and decision-making. They also limit Canadians' ability to access their personal health records and use their personal health information for making decisions about their own health and health care.¹⁶

The use of EHRs does, however, raise notable privacy issues. In a 2001 presentation, the Privacy Commissioner of Canada stated:

If the privacy of health information is not protected by the systems we build, it will be at a dramatic social cost. But this intimate and sensitive information is increasingly being collected, sorted and shared electronically. And as electronic networks, health surveillance systems, and new information and communication technologies advance, the possibilities for violations of privacy multiply. We're approaching a point where patient privacy and any real expectation of confidentiality could well vanish. And it's no exaggeration to fear that lack of confidence in the privacy of health information could lead people to avoid seeking treatment. ... The potential consequences of that are staggering- for ourselves as individuals, for the health care system, for society as a whole.¹⁷

An essential element of privacy protection is to ensure that only key elements of an individual's health information are included in the EHR. Privacy is protected by placing limitations on what can and cannot be included in the EHR. For example, the Australian EHR was designed so that patients are able to control the information placed into the EHR.¹⁸ Important factors such as an individual's ability to exert some control over who accesses information is not contemplated in the *ATIPP Act*. If an EHR is implemented in the NWT, more specific rules to govern its application and confer control to individuals, is likely to improve public confidence and healthcare generally.

¹⁶ (Canada, Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada- Final Report* (Saskatoon: 2002) (Chair: Roy G. Romanow, Q.C.) at 112.

¹⁷ (Privacy Commissioner of Canada, *Condition Critical: Health Privacy in Canada Today, 2001* (Toronto: Privacy Commissioner of Canada, 18 June 2001).

¹⁸ T.D Gunter and N.P. Terry, *The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions*, (2005) 7(1) *Journal of Internet Medical Research*.

Research

The provisions in the *ATIPP Act* that govern research would become more focused on health information under a HIA. The Health Privacy Provinces, in their respective legislation, establish a process whereby research involving health information must be first considered by a research ethics board ("REB") before being disclosed by the healthcare providers (that have custody of control of the desired information) to researchers. Such schemes may serve to promote the pursuit of research from both a participant perspective as well as a researcher perspective. In the former case, participants are likely to be more inclined to consent to participate and consent to have their health information disclosed where assurance can be afforded that the research project has been considered by an independent and impartial body, a REB. In the latter case, most researchers who obtain funding from major agencies are required to obtain REB approval as a function of their terms of funding. This REB approval has historically focused on consent to participate in the project, not consent to the disclosure of information.

The issue of consent to disclosure is based upon balancing possible harm caused by lack of privacy with benefits arising from medical research – and is becoming increasingly important to consider. While Canadian courts have yet to rule squarely on the issue, they have placed a high value on the respect for personal privacy and autonomy.¹⁹

By enacting a HIA, legislators can impose obligations on researchers and custodians regarding REB approval from consent to disclosure perspective as well as impose obligations on REBs as to consideration of consent to information sharing in addition to consent to participation. Doing so may have the effect of creating a more robust REB approval process, and one that participants, researchers, and funding agencies may have greater confidence in. Greater confidence often yields a greater investment of resources, in effect causing more viable and attractive research output. In the research realm, volume and variety of data is pivotal:

...the ability to conduct health research, particularly research on health services and population data, depends heavily on large volumes of readily-accessible, existing data. Such data may include information derived from: personal interviews; analyses of tissue samples; results of scientific tests; physician, hospital, and laboratory records; birth and death records; billing and employee records...Such existing data are often found to be extremely useful for identifying and understanding problems, as well as for providing potential solutions.²⁰

¹⁹ Timothy Caulfield and Nola Ries, "Consent, Privacy and Confidentiality in Longitudinal, Population Health Research: The Canadian Legal Context" (2004) *Health Law Journal Supplement*.

²⁰ (CIHR, *Secondary Use of Personal Information in Health Research: Case Studies*, (Ottawa: Public Works and Government Services Canada, 2000) at 8).

Building on the NWT's potential to participate in, or lead research initiatives, serves the general advantage of increasing credibility and desirability, from both an academic perspective as well as a more general economic perspective. Thriving research programs in the NWT may be a key factor in helping recruit and retain specialized healthcare providers. Further, a HIA could serve to harmonize and streamline, for research involving health information, regulation in the GNWT over research as is currently prescribed under the *Scientists Act*²¹ and the *Medical Professions Regulations*.²² Also specific to the NWT context, it is possible that Aboriginal communities may assert the right to control their own personal information, and not have non-Aboriginal researchers determine appropriate uses, regardless of the legitimacy of research aims. To this end, a HIA with carefully tailored provisions can serve to offer control while still encouraging research activities.

IV. LEARNING FROM HEALTH PRIVACY PROVINCES

As noted above, the Health Privacy Provinces have enacted health specific legislation to address concerns related to the privacy, confidentiality, and use of health information. Accordingly, a review of these pieces of legislation can be instrumental in considering how the GNWT could structure its HIA.

General

In general, these pieces of legislation provide for individually identifying patient information to be released only on the patient's consent or to provide necessary health services. In so doing, greater discretion is afforded to those with a legitimate claim to manage a patient's health information (creating what is often referred to as the "Circle of Care" or "Controlled Arena") while more defined and robust restrictions on movement of information outside the Circle of Care are established. Patients are also given the ability to review or obtain a copy of their personal records, and to request that corrections be made to their records. All of the pieces of legislation provide penalties for failure to comply with the legislation, and confer rights of review and investigation on the part of the oversight body (Information and Privacy Commissioner in Alberta, Saskatchewan and Ontario, and the Ombudsman in Manitoba.) While these pieces of legislation have many similarities, each differs slightly in its scope, coverage and nomenclature.

Alberta

In Alberta, the *Health Information Act* was passed on December 9, 1999 and proclaimed in force in 2001. The entities governed by the Act are referred to as "custodians" and employees, volunteers, contractors or agencies under contract to the custodians are referred to as "affiliates". At this point, the Act only controls information collected or

²¹ R.S.N.W.T. 1988, c.S-4, s.2.

²² R.R.N.W.T.1990, c.M-5, s.6.

produced in the provision of services paid for by the public health care system, with the exception of pharmacists. Health information is defined in a way that limits it to information that is written, photographed, recorded or stored in some manner in a record. The definition of the health information also includes, in addition to "diagnostic, treatment and care information" and "registration information" (which both pertain to patients), certain information about healthcare providers, namely "health services provider information".

Saskatchewan

The Saskatchewan *Health Information Protection Act* was proclaimed in force in 2003. The Act governs the actions of "trustees" who are defined persons with custody or control of personal health information. The Act covers a range of public and private health care activities. For example, service providers engaged by health information trustees are covered by the legislation, whether those service providers are public or private entities. Personal health information protected by the Act is not limited to recorded information, but may include either recorded or non-recorded information.

Manitoba

The *Personal Health Information Act* in Manitoba was the earliest Canadian legislation enacted to protect health information. The Act was proclaimed in force in 1997. The legislation applies to "trustees" who are defined by the Act as health professionals, health care facilities, public bodies, or health services agencies that collect or maintain personal health information. Due to the nature of individuals and entities considered to be trustees, the Act covers both public and private activities. Manitoba limits the protection provided by the Act to recorded information about an identifiable individual that relates to their health, health care history, provision of care or payment for care.

Ontario

Ontario's legislation, the *Personal Health Information Protection Act*, came into force in 2004. The Act covers the collection, use and disclosure of information by "health information custodians", non-health information custodians who receive personal health information from health information custodians and "agents" acting on behalf of health information custodians. The definition of "health information custodian" explicitly includes public and private medical providers, including private hospitals and pharmacies. "Personal health information" protected by the Act explicitly includes both recorded and oral information.

V. SOME ISSUES FOR CONSIDERATION

With the benefit of understanding the various models of legislation enacted by the Health Privacy Provinces, the following are some of the issues that will need to be considered in the development of health specific privacy legislation for the NWT.

Public/Private Sector

While the majority, if not all healthcare services in the NWT are publicly funded, it is still useful to consider the benefits and disadvantages of a HIA including information managed in the context of private sector healthcare services.

The greatest advantage is that if private sector healthcare emerges in NWT, a level of harmony will subsist; that is, health information will not be treated differently if it is managed in a different sector. Given the high value placed on health information generally, legislation, which contemplates such harmonization, is compelling.

A disadvantage is the effort needed to clarify roles with respect to which GNWT Department has the requisite jurisdiction to legislate on matters concerning the private sector. This may have the effect of necessitating more complex consultations and inter-departmental discussions. Note, as a result of commitments to the Standing Committee on Accountability and Oversight, the Department of Justice is examining the implications of developing private sector privacy legislation and reviewing PIPEDA's application in the NWT.

This item should also invite commentary of the practicality and functionality of extending, within the public sector, health information in the custody or control of persons or organizations that may not be directly linked to healthcare services, such as addictions services.

Inclusion of Healthcare Provider Information

Whether the HIA should extend to cover information about healthcare providers also merits consideration.

An advantage to doing so is that this type of information may be incidentally captured in an EHR. If the HIA applies equally to both patient information and healthcare provider information, neither of these types of information need to be separated out or afforded different treatment.

A disadvantage is the possible inconsistency of how GNWT employee information is managed; that is, if personal information about an employee not working in healthcare services is governed under the *ATIPP Act* and personal information about an employee working in healthcare services is governed under a HIA, the rules with respect to each will likely differ. That is because a HIA likely would, in contrast to the *ATIPP Act*, impose more specific safeguarding rules on health information (which would include health service provider information), including restrictions on disclosure to third parties, while at the same time increase availability of such information to individuals within the Controlled Area or Circle of Care. This varied treatment of information may generate a perception of unfairness.

Inclusion of Unrecorded Information

A further scope discussion item worthy of consideration is the application of a HIA to non-recorded information (in addition to recorded information). Recorded information generally includes patient charts and a healthcare provider's written notes, as well as images, photographs, x-rays, maps, drawings or any information that is written, photographed, recorded or stored in any manner.

As non-recorded information would cover oral communications, it may be difficult to track or control. Accordingly, one disadvantage with including non-recorded information is hampered accountability from an internal compliance perspective. On the other hand, the inclusion of non-recorded information may garner greater public confidence, and possibly simplify the application of the HIA, which in turn may encourage compliance.

PIPEDA & Substantial Similarity

The *Personal Information and Protection of Electronic Documents Act* ("PIPEDA") is federal privacy legislation that serves to govern certain organizations (federal works and undertakings "FUBs") as well as fill-in gaps where jurisdictions are lacking private sector privacy legislation. Jurisdictions will not be subject to such a "fill-in" if they enact legislation deemed to be substantially similar to PIPEDA.

There remains debate as to the applicability of PIPEDA in the NWT.²³ However, stakeholder consultation should raise the discussion point of the extent of effort that should be placed on working to draft a HIA that has the greatest chance of being deemed substantially similar to PIPEDA. The benefit of doing so is a decrease in any possible "fill-in" effect, meaning fewer pieces of privacy legislation that govern within the NWT. A disadvantage is that the effort expended may not merit the possible benefit given that PIPEDA nonetheless applies to transborder flows of personal information. Further, such transborder flows are not likely uncommon in the context of healthcare services, particularly if a EHR is adopted that necessitates the flow of health information in and out of NWT.

Oversight & Compliance

Stakeholder consultation will also need to focus on perceived needs for oversight and compliance on two levels. First, on a user level, consideration will need to be afforded to

²³ For example, the website of the Federal Privacy Commissioner of Canada provides: "The situation in the three Territories is somewhat more complex. PIPEDA applies to all federal works, undertakings and businesses (FWUBs) and to the personal information of employees of FWUBs. A FWUB is "any work, undertaking or business that is within the legislative authority of Parliament. Since all organizations in the Territories are considered to be FWUBs, PIPEDA applies to information about employees of municipalities, universities, schools and hospitals in the Territories. However, PIPEDA does not apply to patient or student information in publicly funded hospitals or schools in the Territories because they are not considered to be engaged in commercial activities."

what steps can be practically and successfully implemented to monitor, assess and evaluate compliance at both front line and administrative levels. This would include the use of assessment tools (such as Privacy Impact Assessments²⁴ and the preparation of, and compliance with, supporting policies and procedures. Second, from the Privacy Commissioner level, items requiring discussion include possible role changes; to this end, a wide variety of approaches, based in part on privacy legislation models used in other Canadian jurisdictions, could be canvassed and considered.

VI. CLOSING REMARKS

With the benefit of health specific privacy legislation already being enacted in four jurisdictions in Canada, coupled with increasing awareness surrounding the value placed on health information, the GNWT is presented with a unique opportunity to further advance and enhance the provision and administration of healthcare services through enactment of a HIA.

As there are many competing factors, and many inherent risks, to privacy matters, carefully planned and thoroughly executed stakeholder consultation will play a critical role in the continuation of the HIA project, as well as, and more importantly, the success of the HIA in years to come.

²⁴ PIAs are routinely used in other jurisdictions (for example by organizations and privacy consultants), and are mandated by privacy legislation in some jurisdictions, to ensure users of health information (such a user of the EHR) carefully plan and map information flows and take steps to consider all require safeguarding measures. Doing so also helps mitigate against risk of privacy breaches as well as increases public confidence through enhanced accountability.

