

# Nadjiwan Law Office

Barristers & Solicitors

Patrick M. Nadjiwan, H.B.S.W., LL.B.  
Krista M. Yao, B.A. (Econ.), LL.B.

915 Jocko Point Road, RR4  
Nipissing First Nation  
North Bay, Ontario  
P1B 8G5

Ph: (705) 753-9815  
Fax: (705) 753-9795  
e-mail: mail@nadjiwanlaw.ca

July 4, 2008

By E-mail

Assembly of Manitoba Chiefs  
200 - 260 St. Mary Avenue  
Winnipeg MB R3C 0M6

**Attn: Mabel Horton**

Dear Ms. Horton:

**RE: PRIVACY LEGISLATION AND THE MUSTIMUHW HEALTH INFORMATION SYSTEM**

I have been asked to provide my legal opinion on various privacy-related issues that have arisen from the Mustimuhw Health Information System (MHIS) and the Pilot Wait Times Guarantee Pilot Project. This opinion will consist of the following elements:

- Applicability of federal and provincial privacy legislation on First Nations implementing the Mustimuhw Health Information System and the PWTG Pilot Project;
- Review of potential privacy-related restrictions on ability to utilize the system;
- Analysis from the perspective of transferred communities, non-transferred communities, and partially-transferred (integrated) communities;
- Recommendations for dealing with FNIHB resistance.

The following information was provided to me as background for the preparation of this opinion: the Mustimuhw Health Information System Template Policies and Procedures, the Community Health Information System and Electronic Health Record pamphlet, and the Assembly of Manitoba Chiefs / Saint Elizabeth health Care Primary Wait Times Guarantee Project - The IT Solution Privacy Impact Assessment Questionnaire.

My legal background includes over 10 years of work in the area of First Nations health privacy and First Nations OCAP. Some of my work has included assisting the First Nations Information Governance Committee with the Regional Health Survey, the AFN Health and Social Secretariat with NIHB privacy issues, the First Nations Client Registry, the Aboriginal Health Human Resources Inventory, and the Chiefs of Ontario with Panorama. Through this work, I have acquired expertise in addressing the impact of federal and provincial/territorial privacy and

access to information legislation on First Nations and First Nations OCAP. I am also quite familiar with the bureaucratic and policy resistance of FNIHB.

### **Summary and Conclusions**

- ‘Transferred’ First Nations that wish to implement the MHIS (and PWTG) are not subject to any specific privacy legislation. However, because of Manitoba’s *Privacy Act* and the First Nation’s own duties to its members, it must exercise due diligence in the protection of personal information within its control.
- First Nations with ‘Integrated’ or ‘Transitional’ funding are in the same position as ‘Transferred’ First Nations, provided that the First Nation itself is delivering the health services. Even if there are occasional Health Canada employees working within a First Nation-controlled and owned health centre, the situation will remain the same: federal privacy legislation does not apply.
- Neither the federal *Privacy Act* nor the *Personal Information Protection and Electronic Documents Act* applies to First Nations collection, use and disclosure of personal health information related to their delivery of health services.
- Federal privacy legislation – namely, the *Privacy Act* applies only to federal government departments and agencies. Therefore, if Health Canada is operating a health clinic in a community, with its own employees, then it will be subject to the *Privacy Act* and must comply with the *Privacy Act*. According to federal government policy, it must also comply with Treasury Board policies and guidelines related to the *Privacy Act*.
- Regulated health professionals, whether employed by First Nations or by Health Canada, must comply with Manitoba’s *Personal Health Information Act*. In effect, this means that First Nations – while not directly subject to PHIA – must assist and enable their health professional employees to comply with PHIA.
- “Consent” is the basis of all privacy legislation, whether the *Privacy Act*, PIPEDA or PHIA. If a client consents to the collection, use and disclosure of their personal information – no other legal authority is required in order to authorize the use or disclosure. Consent may be express or implied.

### **Mustimuhw Health Information System (MHIS)**

MHIS basically creates an electronic health record for clients, replacing the paper record. According to the Policies and Practices document personal health information is collected from clients and health care providers: "to assist and support in the delivery of quality health care services to individuals and the community. Member specific information/documentation is required to meet the standards of nursing practice, for quality improvement initiatives and to ensure the co-ordination of care within the Health Centre. Non-identifiable aggregate (grouped) data are collected for accountability to the community, to the Assembly of Manitoba Chiefs

under a data sharing agreement in relation to the Patient Wait Times Guarantee Project, and to First Nations and Inuit Health of Health Canada and in support of funding proposals."

One of the primary principles of the MHIS is the recognition and acknowledgement that the First Nation is the steward of the health information. It is held for the benefit of the health clients who are members of the First Nation. The First Nation commits to protecting the privacy of personal information contained within the MHIS, and to protecting the community's interests in relation to the use or disclosure of aggregated data. This is consistent with the principles of First Nations OCAP.

### **Applicability of Privacy Legislation to First Nations in Manitoba**

There is significant confusion regarding the applicability of privacy legislation in the First Nations' context. There seems to be consensus amongst Department of Justice lawyers and First Nations' lawyers regarding applicability - since the various privacy statutes are relatively clear in their jurisdiction and applicability. However, unfortunately this information has not trickled down, particularly to FNIHB administration and to the Health Canada Access to Information and Privacy Branch. In my experience this has often resulted in FNIHB employees giving incorrect or misinformed advice to First Nations regarding applicable privacy laws.

This section will review all of the potentially relevant privacy laws within the federal jurisdiction and within the Province of Manitoba.

Privacy legislation falls into three jurisdictions within Canada:

- The federal government has constitutional jurisdiction over matters of national concern and has thereby enacted 2 pieces of privacy legislation: the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*.
- The provinces have constitutional jurisdiction over property and civil rights, and matters of a local nature. The province of Manitoba has thereby enacted the (provincial) *Privacy Act*, the *Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Act*.
- First Nations have the inherent right to self-governance and thereby have authority to enact their own privacy laws and regulations. To my knowledge none of the First Nations participating in the MHIS has yet implemented their own privacy law. If any First Nation does have its own privacy law, naturally, the MHIS would have to be reviewed to ensure that the participating First Nation complies with its own laws.

The following chart details the privacy laws for Canada and Manitoba, who the law applies to, and how each law impacts upon the MHIS.

## Federal Legislation

|   |   |
|---|---|
| Statute   | <b>Privacy Act</b> , R.S.C. c. P-21   |
| Description/Summary                                     | The purpose of this Act is to regulate the collection, use and disclosure of personal information by government institutions, and to provide individuals with a right to access their own information.  |
| Who Does it Apply To                                    | <p>The Act applies <u>only to federal government departments and institutions</u>, as listed in the Schedule to the Act.</p> <p>The Act <u>does not apply to First Nations or First Nations-controlled organizations</u>. However, the federal government, through contribution agreements often tries to have organizations adopt personal privacy policies comparable to the <i>Privacy Act</i>.</p>  |
| What Records Does it Cover                              | The Act covers only identifying personal information (not community-level information) up to 20 years following the death of the individual.  |
| Potential Impact on First Nations implementing the MHIS | <p>Because the <i>Privacy Act</i> only applies to federal government departments (i.e. FNIHB) it will only impact the MHIS <u>if</u> FNIHB is directly delivering the health service. In other words, in non-transferred communities, where FNIHB directly delivers health services, FNIHB must comply with <i>Privacy Act</i> requirements if the First Nation wishes to participate in the MHIS.</p> <p>For transferred First Nations, the <i>Privacy Act</i> does not apply to the First Nation's delivery of health services, or to their participation in the MHIS.</p> <p>In circumstances where the First Nation delivers health services directly, but where there may be a Health Canada employee seconded or otherwise contracted to assist the First Nations' health services delivery, the <i>Privacy Act</i> still <u>will not apply</u>. The federal <i>Privacy Act</i> applies only to federal departments and institutions. It does not apply to federal employees who are working for First Nations.</p> |

|                      |   |
|----------------------|---|
| Statute              | <b>Personal Information Protection and Electronic Documents Act</b> , R.S.C. c. P-8.6   |
| Description/Summary  | The purpose of this Act is to establish "rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." |
| Who Does it Apply To | <ul style="list-style-type: none"> <li>• Organizations that collect, use and disclose personal information in the course of a commercial activity.</li> <li>• Federal works, undertakings and businesses that collect, use or disclose personal information, including personal information</li> </ul>  |

|   |  |
|---|--|
|   | <p><b>about employees</b> in any province or territory.</p> <ul style="list-style-type: none"> <li>The Act does not apply to the federal government or any agency or institution covered by the federal <i>Privacy Act</i>.</li> </ul>   |
| What Records Does it Cover                              | <ul style="list-style-type: none"> <li>The Act applies to all personal information collected by organizations with commercial activities (including private health care providers, charities who <i>sell</i> donor lists, etc.)</li> <li>The Act also applies to First Nation <u>employers only in relation to their employee records</u>. It may also apply to First Nations if they engage in commercial activities, and in relation to information collected in the course of those commercial activities.</li> </ul> |
| Potential Impact on First Nations implementing the MHIS | Privacy protection in PIPEDA <u>will not</u> apply to First Nations participating in the MHIS because their provision of health services is not a commercial activity.   |

## Manitoba Legislation

|   |  |
|---|--|
| Statute   | <b>The Privacy Act</b> , C.C.S.M. c. P125  |
| Description/Summary                                     | Manitoba is one of the few provinces which have codified the tort (legal wrong) of “violation of privacy.” It clarifies an uncertain common law by allowing individuals whose privacy has been unjustly violated to sue for monetary damages and obtain other remedies, without proof of actual damages.   |
| Who Does it Apply To                                    | This Act applies to everyone in Manitoba, including First Nations, as a result of s.88 which incorporates provincial laws of general application.  |
| What Records Does it Cover                              | n/a  |
| Potential Impact on First Nations implementing the MHIS | If an individual’s privacy is violated he or she has a legal claim against the individual or organization that is responsible, including a First Nation. This generally creates greater personal privacy protection within Manitoba. It also increases potential liability for anyone who has custody of personal information. Basic privacy protection and due diligence will minimize potential liability. |

|                      |   |
|----------------------|---|
| Statute              | <b>The Personal Health Information Act</b> , C.C.S.M. c. P33.5  |
| Description/Summary  | The Act imposes obligations on trustees for the protection of personal health information, specifically its collection, use, disclosure and security.   |
| Who Does it Apply To | <p>The Act applies to “trustees” who maintain (have custody or control of) personal health information.</p> <p>Trustees under PHIA include:</p> <ul style="list-style-type: none"> <li>all provincial public bodies, including provincial government departments and agencies and local public bodies, educational</li> </ul> |

|   |   |
|---|---|
|   | <p>bodies (such as school divisions, universities and colleges), health care bodies (such as hospitals and regional health authorities), and local government bodies (such as the City of Winnipeg, municipalities, local government districts, planning districts and conservation districts; universities and colleges);</p> <ul style="list-style-type: none"> <li>- health professionals licensed or registered to provide health care under an Act of the Legislature or who are members of a class of persons designated as health professionals in the Regulations (such as doctors, nurses, physiotherapists, psychologists, etc.);</li> <li>- health care facilities (such as hospitals, personal care homes, psychiatric facilities, medical clinics, laboratories, The Manitoba Cancer Treatment and Research Foundation, and community health centres or other health care facilities designated in the regulations); and,</li> <li>- health services agencies providing health care under an agreement with another trustee (such as the Victorian Order of Nurses).</li> </ul> <p>While it does not apply specifically to First Nations who are delivering health care services, it does apply to regulated health professionals who are employed by First Nations, or who are employed to work in First Nation communities by Health Canada.</p> |
| What Records Does it Cover                              | <p>The Act covers “personal health information” which is defined as information that relates to:</p> <ul style="list-style-type: none"> <li>- the individual's health, or health care history, including genetic information about the individual; or,</li> <li>- the provision of health care to the individual, or payment for health care provided to the individual;</li> </ul>   |
| Potential Impact on First Nations implementing the MHIS | <p>This Act requires consent for the release of personal health information held by a “trustee” unless the use or disclosure falls within one of the exemption categories contained in the Act.</p> <p>The MHIS Practices and Policies document indicates that personal health information will only be disclosed with client consent, or as required by law, or to other health providers for the purpose of the client’s health. This is consistent with PHIA.</p>  |

### **The MHIS Participants**

From a privacy perspective, the relevant participants in the MHIS and PWTG Pilot Project will include: the First Nation, health professionals, clients; and potentially, Health Canada (FNIHB) and Saint Elizabeth Health Care.

**The First Nation:** As described in the legislative review, above, First Nations are not subject to any federal privacy legislation in relation to the MHIS. First Nations are also not subject to Manitoba's *Personal Health Information Act* (PHIA) since First Nations are not categorized as "trustees" under the Act. Likewise, First Nations are not subject to Manitoba's *Freedom of Information and Protection of Privacy Act* which only applies to the provincial government and other provincially-regulated public bodies within Manitoba.

However, as a law of general application Manitoba's *Privacy Act* will apply to First Nations along with everyone else in Manitoba. Thus, First Nations participating in the MHIS must satisfy themselves that they are not "unjustly violating" anyone's personal privacy rights. Manitoba's *Privacy Act* does not contain any specifics on what would constitute an "unjust violation". Therefore, we would first look to the "due diligence" provisions of the Policies and Procedures and the fact that a Privacy Impact Assessment has been conducted in accordance with provincial PHIA standards. These elements will create the framework for personal privacy protection and assuming that the First Nation complies with the policies, etc, that would address and minimize any potential liability under Manitoba's *Privacy Act*.

In addition to compliance with statutes, participating First Nations must be mindful of their contractual liabilities to Health Canada via the Consolidated Contribution Agreements. Section 17(1) of the current Set Funding CCA and section 20(1) of the Transitional Set Funding CCA states:

The Recipient shall ensure that all information of a personal medical nature to which the Recipient or its officers, servants or agents becomes privy pursuant to or as a result of this Agreement, shall be treated as confidential and not disclosed to any person except with the consent of the individual(s) to whom the information relates, or otherwise in accordance with applicable law.

Since there is no applicable law (other than Manitoba's *Privacy Act*), this provision would be interpreted to mean that First Nations ('recipients') require client consent (or other legal authority) to disclose any personal information within the MHIS, or else potentially be in violation of the CCA. This would not, obviously, constitute a violation of any law, but a potential breach of an agreement. However, the repercussions from breaching the CCA could be equally dire for First Nations.

The limitations of the CCA should not be any concern to First Nations participating in the MHIS because according to the section 1(4) of the template Policies and Practices, personally-identifying information will only be disclosed:

- With written member consent; (This is referred to as "express consent".)
- To comply with a subpoena, warrant or order; (This is disclosure in accordance to applicable law.)
- To comply with a statutory mandate such as the Child, Family and Community Services Act or Part 4 (Disease Control) of the Public Health Act; (Again, in accordance with applicable law.)
- With other health service providers if the information is necessary to ensure safe, effective and continuous care or treatment on a "need to know" basis; (This is considered "implied consent" - see more on consent below.)

**Health Professionals:** Regulated health professionals in Manitoba fall within the jurisdiction of PHIA, as described in the charts above. This means that while First Nations themselves are not required to comply with PHIPA, the health professionals that they employ are. Likewise, because health professionals are provincially-regulated, even health professionals employed by Health Canada/FNIHB to deliver health services to First Nations would fall under PHIA. Therefore, health professionals in transferred and non-transferred communities must comply with PHIA.

Thus, in order for these health professionals to be in compliance they must be satisfied that their participation in the MHIS meets the requirements of PHIA. Completion of the Privacy Impact Assessment questionnaire is the first step to ensure that requirements are met. Health professionals should also be familiar with their ongoing privacy obligations under PHIA to maintain compliance.

**Saint Elizabeth Health Care:** According to the documentation provided, First Nations participating in the MHIS will share aggregate data with Saint Elizabeth Health Care for the purpose of the Patient Wait Times Guarantee Project. Because the information shared will be aggregate data, there are no privacy restrictions on the data sharing. However, if this situation changes and personal health information is shared by First Nations with Saint Elizabeth Health Care, you will have to ensure compliance with PHIA.

**Health Canada - FNIHB:** Health Canada has two potential roles within the MHIS. First, there is an expectation that some aggregate health data may be shared with Health Canada for project or funding purposes. Since aggregate data does not contain personal identifiers, it is not subject to any privacy legislation and there is no restriction on Canada's ability to collect, use or disclose such data.

Second, Health Canada, through FNIHB may be delivering health services directly within non-transferred communities. The health services are delivered by Health Canada employees. These employees face a dual regulatory scheme because the federal *Privacy Act* will apply in their capacity as government departments. Thus, failure to comply may jeopardize the employees' job security. However, PHIA will also apply to the individual health professionals employed by Health Canada because the health professionals are provincially-regulated. Thus, failure to comply with PHIA may jeopardize their professional license.

When comparing both PHIA and the federal *Privacy Act* it is evident that PHIA provides substantially greater privacy protection for personal health information than *the Privacy Act*. The *Privacy Act* actually gives FNIHB very broad authority to use and disclose First Nations' personal health information without consent, provided that the use or disclosure is "consistent with the purpose" for which it was collected. This "consistent use" category is usually interpreted very broadly by FNIHB in order to justify almost any departmental use. PHIA is significantly more restrictive on the use of personal health information.

While the above discussion deals with legal compliance, the federal government has also created its own policies on how it will ensure compliance with the *Privacy Act*. Treasury Board policy thus adds an additional layer of bureaucratic requirements that if followed, presumably, assure the federal department that it has complied with the *Privacy Act*. One of these requirements is that a privacy impact assessment be conducted if a proposal involves any of the following:

- a new or increased collection, use or disclosure of personal information, with or without the consent of individuals;
- a broadening of target populations;
- a shift from direct to indirect collection of personal information;
- an expansion of personal information collection for purposes of program integration, program administration or program eligibility;
- new data matching or increased sharing of personal information between programs or across institutions, jurisdictions or sectors;
- development of or a new or extended use of common personal identifiers;
- significant changes to the business processes or systems that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information; or
- the contracting out or devolution of a program or service to another level of government or the private sector.

Based upon my review of the documentation, the MHIS is simply going to involve the conversion of existing paper records into an electronic record. The database will be maintained at a local level, within the First Nation community. More importantly, personal information will not be disclosed outside of the "circle of care" for the client without consent or other legal authority. In other words, the MHIS does not contemplate any increased collection, use or

disclosure of personal information. Therefore, I would argue that FNIHB should not require a PIA for non-transferred communities to participate in the MHIS.

### **The Role of Consent**

All privacy legislation is fundamentally based upon client consent. Personal information can be collected, used and disclosed as long as the individual provides their informed consent. Most privacy statutes then describe the special situations or circumstances when personal information may be used or disclosed without consent. Statutes typically also contain other incidental provisions such as: minimizing the retention period, requiring destruction of personal information that is no longer useful, and permitting individuals to access their own personal information. However, the bulk of all privacy statutes involve giving legal authority to data holders to use or disclose personal information without consent. As stated in the Treasury Board Policy on Privacy Protection:

The consent of the subject individual allows institutions to use or disclose personal information for any purpose consented to by the individual. In other words, the consent of the individual removes the need to find a provision [under the *Privacy Act*] for use or disclosure.

Consent can also be express or implied. Express consent exists where a specific act of an individual indicates their consent; generally a written or verbal indication of acceptance. Implied consent arises where consent may reasonably be inferred from the action or inaction of the customer. For example, if a client gives their personal information to a health professional, he or she is impliedly consenting to that information being recorded onto their chart and used for purposes consistent with the provision of health services, which would include billing purposes. For this reason, assuming that MHIS remains consistent with the current Policies and Practices template, participating First Nations would be able to rely upon either express or implied consent. In fact, the MHIS is based upon individual and community consent.

When dealing with aggregated (non-identifying) information, client consent is not an issue and is not required, provided there is no reasonable way to use the aggregated information to re-identify any individual, thus breaching personal privacy. However, while individual consent is not required to use or disclose aggregate data, OCAP principles mandate that community consent be obtained. According to the Policies and Practices of the MHIS, community consent will be required for disclosure. As a result, the MHIS provides protection for aggregate First Nations' data, where the federal *Privacy Act* does not and cannot.

### **FNIHB Resistance**

As mentioned above, in my experience many Health Canada employees, either intentionally or mistakenly, advise First Nations that the *Privacy Act* applies to First Nations. If they would only take the time to closely read the *Privacy Act*; or to consult either their own legal counsel or the Office of the Privacy Commissioner of Canada they would realize that the *Privacy Act* only applies to federal government departments and agencies. Yet there appears to be some sort of bureaucratic or policy reticence on the part of Health Canada that results in these obstructive misunderstandings and misrepresentations. In the case of the MHIS, this may be a reason for some of FNIHB's resistance to this project.

Based upon my previous discussion with Tracy Scott and my own experience dealing with FNIHB I expect that there are at least three objections that FNIHB is posing to First Nations who wish to participate in the MHIS:

1. For non-transferred communities where FNIHB provides health services, FNIHB may claim that they cannot use the MHIS because it does not comply with the *Privacy Act*.

In fact, because the MHIS is based upon client and community consent, and simply changes the manual record keeping into an e-health record, with the data maintained in-house, there are no legal obstacles associated with *Privacy Act* compliance. FNIHB would have to satisfy itself that the privacy policy and security mechanisms surrounding the MHIS are acceptable under Treasury Board Policy – however, this should not be a significant burden. Moreover, this is a First Nation-driven initiative that meets provincial privacy standards under PHIA and which is intended to address some of the deplorable health discrepancies between First Nations and the rest of Canada. Given FNIHB's lack of results in the area, and its fiduciary duties in relation to First Nations' health this should be seen as a positive step. Moreover, by refusing to participate in the MHIS, FNIHB is denying First Nations the ability to tap into the benefits of e-health records, and the corresponding benefits to individual health care and community health. Forcing First Nations to continue with traditional paper records over the long term, while the rest of society moves towards e-health records will only increase existing health discrepancies and ensure that First Nations cannot progress.

At the outset, you would have to approach FNIHB at a policy and technical level to determine what their precise concerns are. If they have privacy problems, it may be appropriate to recruit the assistance of the federal Privacy Commissioner. If the problem is FNIHB indifference or just refusal to respond, the problem may have to be elevated to a higher level within FNIHB – and perhaps to a political level.

2. FNIHB may claim that its employees working within integrated or transferred communities (but working within a First Nation-controlled and owned health centre) are still subject to the *Privacy Act* with the same result as above.

This position is based upon a misinterpretation of the *Privacy Act*. One solution is to contact the Office of the Federal Privacy Commissioner to confirm that the *Privacy Act* applies to organizations (federal departments and agencies) and not individuals. Thus, if a First Nations' employee is somehow seconded to work at Health Canada, the employee will have to comply

with the *Privacy Act*. But if a Health Canada employee is somehow seconded to work for a First Nations' health authority, the *Privacy Act* does not apply.

Another option to consider is that if a FNIHB employee working under the direction and instruction of the First Nation refuses to participate in the MHIS, and the employee is a health professional, you could consider reporting the employee to his or her professional regulatory association (the College of Nurses of Manitoba, etc.). If an individual has consented for their information to be input into an e-health record and the health professional refuses, this may constitute a breach of professional obligations.

3. FNIHB may claim that the *Privacy Act* applies to transferred First Nations and that the First Nation cannot participate in the MHIS without FNIHB's approval.

This is entirely incorrect. The *Privacy Act* does not apply to First Nations and FNIHB approval is not required for a First Nation to participate in the MHIS. However, the consolidated contribution agreements for transferred and integrated/transitional First Nations require client consent for disclosure of personal health information. Since MHIS is based upon client consent (implied and/or express), this presents no legal obstacle. FNIHB has no role here and cannot prevent transferred First Nations from participating in the MHIS.

That concludes this legal review. If there are any questions, or if you would like any follow-up to this work, please feel free to contact me.

Sincerely,

Nadjiwan Law Office

Digital Signature  


Per: Krista M. Yao  
[krista@nadjiwanlaw.ca](mailto:krista@nadjiwanlaw.ca)