Privacy Tool Kit

Information to share from the First Nations Centre of the National Aboriginal Health Organization (FNC@NAHO)

THE NUTS AND BOLTS OF PRIVACY

Introduction

What Privacy Means to First Nations

What are the Gaps

What is OCAP

What's Out There

What You Can Do

Glossary

Privacy Resources

A Model Privacy Code

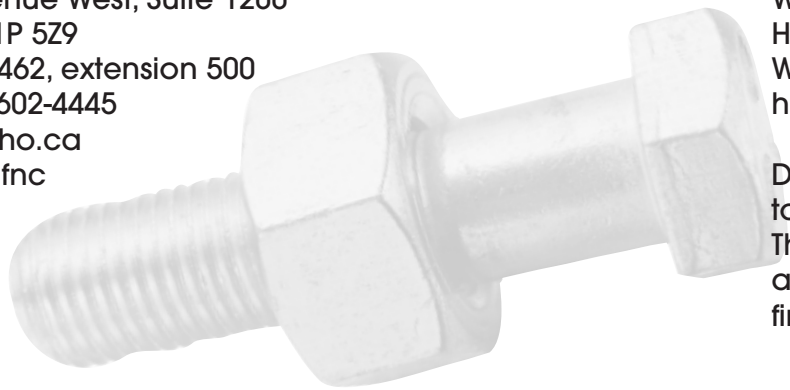
We have assembled this creative kit of information for you on the **Nuts and Bolts of Privacy**. We hope it will assist you by providing the latest information on an issue that is increasingly important to First Nations. This is particularly the case with the increased use of computers, Internet technology, information-gathering initiatives, sharing of information, access and consent to information, and new privacy legislation.

This Privacy Tool Kit is one of several information packages being prepared by the First Nations Centre (FNC) of the National Aboriginal Health Organization (NAHO) to inform and share knowledge on key issues and to assist in community capacity building. We have prepared this kit by drawing on presentations and materials that experts in the fields of privacy, law, ethics, and First Nations health information have shared at various workshops and information forums co-ordinated by NAHO.

Similar tool kits offered by the FNC cover the following topics: Health Surveillance: The Basics, Understanding Research and Ethics in Health Research: Key Issues.

If you have questions or comments about this Tool Kit, please contact us:

First Nations Centre
220 Laurier Avenue West, Suite 1200
Ottawa, ON K1P 5Z9
Tel: (613) 237-9462, extension 500
Toll-free: 1-877-602-4445
E-mail: fnc@naho.ca
www.naho.ca/fnc



First, we need to ask the question—what is privacy? We understand privacy as the right of an individual to control who has access to his or her personal health information, and under what circumstances. Privacy also means the "right to be left alone" and is linked to the fundamental human right of freedom and personal autonomy.

Privacy can be an issue for individuals. But privacy can also be a concern for groups of individuals, such as First Nations communities or reserves, which are often severely affected because of their small population size. First Nations people are among the most "counted" people in Canada because so much information gathering and tracking take place on each and every individual in our communities. The collection of administrative data on individuals in the areas of health, education, employment, income, band numbers, housing, and children, etc. is occurring on a daily basis.

First Nations people can ask the following questions about their personal health information:

Who is collecting it?
Where is it being sent?
Who is it being exchanged with?
How is it stored?
Who has access to it?
Who has control over it?
Who owns it?
How long is it being stored for?
What privacy legislation (federal/provincial/territorial) impacts health information on- reserve?

Do First Nations individuals in the communities know the answers to these questions? Unfortunately, the answer is most likely "no." The majority of our people may not know where to go to get the answers to these questions. This Tool Kit will, hopefully, act as a first step.

Overall, First Nations lack general knowledge on what their individual privacy rights are, and what protections are in place for their community privacy rights.

Do you know...?

Do you know who has access to your personal records within government and community facilities?

Do you know that the *Privacy Act* and the *Access to Information Act* apply in non-transferred community health facilities? Do you know that in these facilities - although the *Privacy Act* can protect your personal information—general information on health conditions in the community can be accessed by someone making a request to government?

Do you know that you can make a complaint to the Privacy Commissioner of Canada regarding how the federal government handles your personal information?

Do you know that the new law called the *Personal Information Protection and Electronic Document Act* (PIPEDA) does not protect your personal information held in your community unless this information was collected to support a commercial activity?

Do you know that nurses working in Manitoba, Saskatchewan, Ontario and Alberta have to protect your personal information in accordance with the health information acts in these provinces?

Do you know that in transferred community health facilities, there is no protection for personal information beyond professional codes of conduct and regulations for health professionals, with the exception of five provinces (Manitoba, Alberta, Saskatchewan, Ontario and Quebec)?

Do you know what professional codes of conduct nurses must comply with when they handle your personal information?

Do you know that your Band Council can pass a law to protect the privacy of both personal information and community information in a way that matters to your community?

Looking at the **"What's Out There"** drawer of your Tool Kit, you can already begin to identify gaps in the current laws and other protections in place across the country. Just to recap, here are some of the main gaps:

- For non-transferred communities, the government owns the health records, and they are protected under the *Privacy Act* and the Treasury Board of Canada Policy on Privacy and Data Protection. But community-level information "aggregated" from the records - that is, collected but without showing personal identity of individuals - can be accessed if a request is made to the government. This is because the *Access to Information Act* applies in this case. "Access to Information" means that Canadians have the right to look at information that is within the government's control, if they ask.
- For transferred communities, where a community owns the health records, there is no legal protection of these records except for professional regulations and codes of conduct to which nurses, physicians, and other licensed health professionals must comply, as well as health information acts in Alberta, Manitoba, Ontario and Saskatchewan, and constitutional protection in Quebec. Except in Ontario the provincial laws do not apply to health facilities, but to practices of health professionals licensed in those provinces.
- First Nations are not generally consulted on the drafting of these laws and professional codes.
- We do not yet know how these laws, or the issue of privacy, might impact First Nations' treaty rights.

So how can you protect information in your community? Open the next drawer and find out!

The right of a First Nations community to Own, Control, Access, and Possess (OCAP) information about its population is fundamentally tied to self-determination, to influence how the community preserves and develops its culture. If a community acknowledges this OCAP right, it can make decisions on why, how, and by whom information is collected, used, and shared for research, evaluation and planning purposes, and even for patient care. It can also ensure that individual and community privacy is protected in a way that is appropriate to the First Nation's language and beliefs.

The term OCAP was coined by the National Steering Committee of the First Nations and Inuit Regional Longitudinal Health Survey. This is a national health survey process being conducted by the First Nations Centre@NAHO, and regional First Nations organizations under the mandate and direction of the Assembly of First Nations' Chiefs Committee on Health. While the understanding and definition of OCAP continue to take shape and to be debated, it is a set of principles in evolution.

Ownership: The notion of ownership refers to the relationship of a First Nations community to its cultural knowledge/information/data. The principle states that a community or group owns information collectively in the same way that an individual owns his or her personal information

Control: The aspirations and rights of First Nations people to have control of all aspects of their lives and institutions extend to research and information. The principle of control asserts that First Nations people, their communities, and leadership bodies are within their rights in seeking to control all aspects of research and information management processes which impact them.

Access: First Nations people must have access to information about themselves and their communities, regardless of where it is currently held.

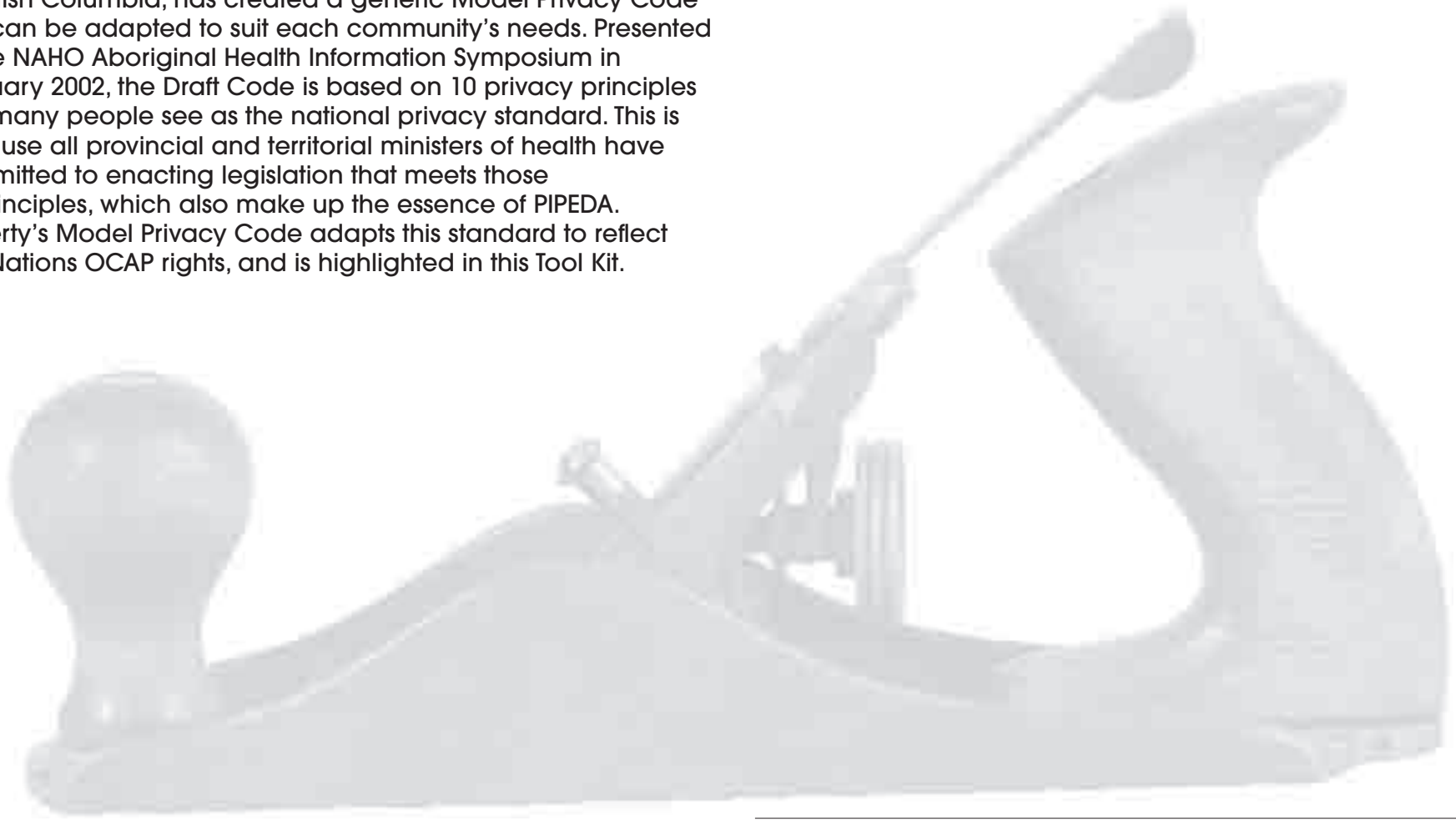
Possession[1]: While ownership identifies the relationship between a people and their data in principle, the meaning of possession or stewardship is more literal. Although not a condition of ownership in itself, possession (of data) is a mechanism by which ownership can be asserted and protected. When data owned by one party are in the possession of another, there is a risk of breach or misuse. This is a particularly important issue when trust is lacking between the owner and possessor.

OCAP is a way to be proactive in the future. It opens up new avenues for the expression of self-determination and self-governance in the areas of research and information, and provides a measure of hope for positive change.

When it comes to privacy, OCAP can be brought to life in community codes or laws. This form of self-regulating becomes especially important when you consider that in most provinces, except for professionals duties owned by regulated health professionals working in our communities, there are no laws that protect personal health information, outside of information within the direct control of the federal or provincial governments. Moreover, there is no law at all that protects community health information. The national *Privacy Act* only protects personal information, and it applies only to federal government activity, such as the practice of nurses who are Health Canada employees. For those provinces with health information privacy acts (such as in Ontario, Manitoba and Saskatchewan) the legislation also just protect personal health information – and not sensitive community information. The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not apply to the health sector unless commercial activity is involved, such as the selling of information for profit.

First Nations communities can also make sure that governments and research partners comply with their privacy codes and codes of ethics through data-sharing and research agreements. For instance, the Carcross Tagish First Nation in the Yukon has created a privacy code that is watched over by a Council of Elders. In addition, David Flaherty, former Privacy Commissioner of British Columbia, has created a generic Model Privacy Code that can be adapted to suit each community's needs. Presented at the NAHO Aboriginal Health Information Symposium in February 2002, the Draft Code is based on 10 privacy principles that many people see as the national privacy standard. This is because all provincial and territorial ministers of health have committed to enacting legislation that meets those 10 principles, which also make up the essence of PIPEDA. Flaherty's Model Privacy Code adapts this standard to reflect First Nations OCAP rights, and is highlighted in this Tool Kit.

Awareness of OCAP has increased in the last few years among First Nations leaders, health care workers and communities, but also within government. We have become aware that information is power, and with that power comes responsibility to make good, informed decisions about how our information, both individual and collective, is protected.



1 The "P" (Possession) was added to "OCA" following a legal review by Krista Yao (Nadjiwan Law Office), that highlighted how statistical information in the government's possession is readily accessible through Access to Information requests irrespective of ownership or written agreements.

Here's a look at various forms of protection of your personal health information that are out there right now. They are divided by jurisdiction.

First Nations Organizations and Communities	Government of Canada	Provinces/Territories	Other
• Band Council Resolutions or laws • Court cases • Treaties • Contracts and data-sharing agreements • Privacy codes or policies (NAHO has one.) • Privacy Impact Assessment of the First Nations Regional Health Survey • First Nations Information Governance Committee • Aboriginal Health Infostructure Sub-Committee on Privacy	• *Privacy Act* and Treasury Board of Canada Privacy Policy • *Access to Information Act* • Privacy Commissioner of Canada • Treasury Board's Privacy Impact Assessment Policy • Health Canada's Privacy Impact Assessment • Health Canada's Personal Information Banks documented in Info Source • Health Canada's First Nations and Inuit Health Branch Program Privacy Assessment Requirements and Reviews • The First Nations and Inuit Health Branch Privacy Code	• Health Information Acts in Alberta, Manitoba, Ontario and Saskatchewan • Québec Constitution • British Columbia *Personal Health Information Act* • Colleges of Health Professions, B.C. Personal Information Act	• Contracts between parties • Canadian Organization for the Advancement of Computers in Health Security and Privacy Guidelines • Canadian Standards Association Model Code for the Protection of Personal Information • Canadian Institute for Health Information Privacy Code • Other private sector codes and policies

Common to Government of Canada, Provinces and Territories

Personal Information Protection and Electronic Documents Act (PIPEDA)
F/P/T Harmonization Resolution on the Protection of Personal Health Information
Both of the above documents are based on the 10 Privacy Principles.

What does legislation do to protect your health information?

Legislation regulates the collection, use, disclosure, and destruction of personal health information. One of the bases of all legislation is that personal health information cannot be collected, used, or disclosed without the consent of the client.

However, there is no protection over information that is not identifiable to a particular individual (i.e. anonymous data, or data which have had personal identifiers removed).

No (non-Aboriginal) government within Canada recognizes community privacy rights or interests through legislation. How can you protect community privacy interests/rights?

- Respect OCAP principles.
- Enact First Nation laws, which recognize and protect community privacy rights.
- Ensure that all agreements with third parties address community privacy rights.
- Because of vulnarability to Access to Information Act requests, do not allow the federal government to have control over any data/info where there are community privacy interests.

Access to Information Act
Because the federal *Privacy Act* does not protect non-identifying(KMY2) data, these data are accessible by anyone under the *Access to Information Act*. All such non-identifying data within the control of the federal government are therefore available to the public.

There are some exemptions that permit the federal government to withhold the release of information (i.e. national security, economic/financial interests), but generally none would apply in a First Nations health context.

A Plan of Action for protecting health information in your community

How can you protect health information in your community? These simple steps can help you to define rules for the collection, use, sharing, and safekeeping of information. As you can see from the table below, each step corresponds to one of the 10 privacy principles, but also grounds them in the day-to-day realities of a First Nation health facility. This **PLAN OF ACTION** can lead to the creation of Guidelines that could be transposed in a **Band Council Resolution** and appended in **contracts** with government, researchers, provincial/territorial health organizations, or any other group that would want to access your community's health information. Resolutions and contracts are ways to enforce compliance within and outside your community with the rules you have defined.

To see an example of Guidelines, see the chart in this section.

STEP 1: IDENTIFY WHO IS RESPONSIBLE

Much of First Nations information is in the hands of people and organizations that do not have to answer to First Nations.

In your community, identify someone, or a group of individuals with a strong commitment to the community, who can take responsibility for ensuring that your First Nation owns, has control over, and adequately protects its health information. Possibilities include the community health director, a privacy board, or a Council of Elders.

Demonstrating that your community has the capacity to address the issue of privacy will support the transfer ("taking over") of initiatives run in the past by non-First Nations groups, such as research and public health planning. Identifying a privacy contact person is also a requirement of Ontario's *Personal Health Information Protection Act*.

STEP 2: IDENTIFY WHY INFORMATION WILL BE COLLECTED

Make a list of the purposes for which health information is collected. Inform clients of the purposes for collecting personal information; and inform the community and leadership of the purposes for collecting community information. Make sure they understand them.

STEP 3: OBTAIN CLIENT CONSENT AND COMMUNITY CONSENT

Make sure that everyone knows what is happening with their personal health information, and the community-level health information that they agree with the collection, use, and sharing of their health information before this takes place. If information is to be used for a purpose that you did not identify before, make sure that they agree to this new purpose before using the information.

Sometimes, you will not be able to gain the client consent of community members, such as in special security, legal, or medical cases. Also, you may not need to get written or verbal consent of community members in cases where their consent is considered as implied. For example, if a person comes to see the nurse about a headache, it is reasonable to assume that he/she agrees to the nurse writing information in the patient chart. Where provincial privacy legislation applies, you must become familiar with the circumstances where implied consent can not be used, and likewise, where consent is not required.

For non-identifying information, which nonetheless identifies the community (although not the individual), obtain First Nation consent for use, access or disclosure.

Make sure that you provide community members with a way to withdraw their consent at any time, and also let them know about any possible impact if they do so.

STEP 4: SET LIMITS ON COLLECTING INFORMATION

Be clear about what your community wants and doesn't want from health information on its members. Collect information only for the purposes you listed in Step 2. Collect this information only in a way that is fair to clients and compliant with the law. Be open and honest with community members.

STEP 5: SET LIMITS ON USING, SHARING, AND SAFEKEEPING INFORMATION

Allow health information to be used and shared only for the purposes listed in Step 2 or as required under applicable provincial health privacy information. If you are transmitting health information to third parties, including FNIHB, be aware of FNIHB intended use for the information and FNIHB privacy practices. Keep the information only for as long as it is needed and establish minimum and maximum periods for the general safekeeping of information. Make sure you have given enough time for clients to access their personal health information, especially if this information was used to make a decision about them. For non-personal community information, obtain First Nation consent prior to using, sharing or disclosing community information outside of the community.

Create procedures to identify when a use or disclosure is beyond what is described in your plan of action or written privacy statement, and what to do in the circumstances. Take steps to protect personal and community health information that you transfer to others (for example, including privacy clauses in your contracts with agents).

STEP 6: ENSURE THAT INFORMATION IS ACCURATE

Take care to keep information as accurate, complete and up-to-date as possible. This is important to prevent wrong or incomplete information being used to make a decision about a community member.

STEP 7: ENSURE THAT INFORMATION IS SECURE

Develop and follow security practices to protect health information against theft, loss and unauthorized access, copying, modification, use or disclosure from within or outside the organization. this can be done by putting in place:

- physical security such as locked file cabinets
- organizational security, such as security checks on employees, and employee training on privacy and security
- technological security, such as passwords.

Conduct Threat Risk Assessments on a regular basis to verify whether the security measures are adequate to protect the health information.

STEP 8: INFORM COMMUNITY MEMBERS OF THIS PLAN OF ACTION

Share with your community members this Plan of Action, and any guidelines and procedures that you create to support the Plan. Seek their advice, especially support from Elders and community champions. Educate your leadership concerning the importance of privacy. Build on your success and collaborate with other First Nations to learn from them, and share your experience. B.C. and Ontario privacy legislation requires you to develop and make available a written statement on your information practices.

STEP 9: PROVIDE COMMUNITY MEMBERS WITH ACCESS TO THEIR PERSONAL INFORMATION

Assist community members when they ask for access to their personal information. In some special cases, because of legal, security or other reasons, you may not be able to grant them this access. When this happens, let them know why.

Let your community members know from where their personal information has been collected, and with whom it has been shared.

Allow them to ask for changes to the information if they feel it is not accurate or complete and make these corrections if appropriate.

STEP 10: ASSIST COMMUNITY MEMBERS IN ASKING QUESTIONS AND MAKING COMPLAINTS

Let community members know to whom, and how, they can present their questions and make complaints. Make sure their questions and complaints are addressed. Have a clear procedure for looking into their complaint and for responding to it, whether or not it is found to be justified.

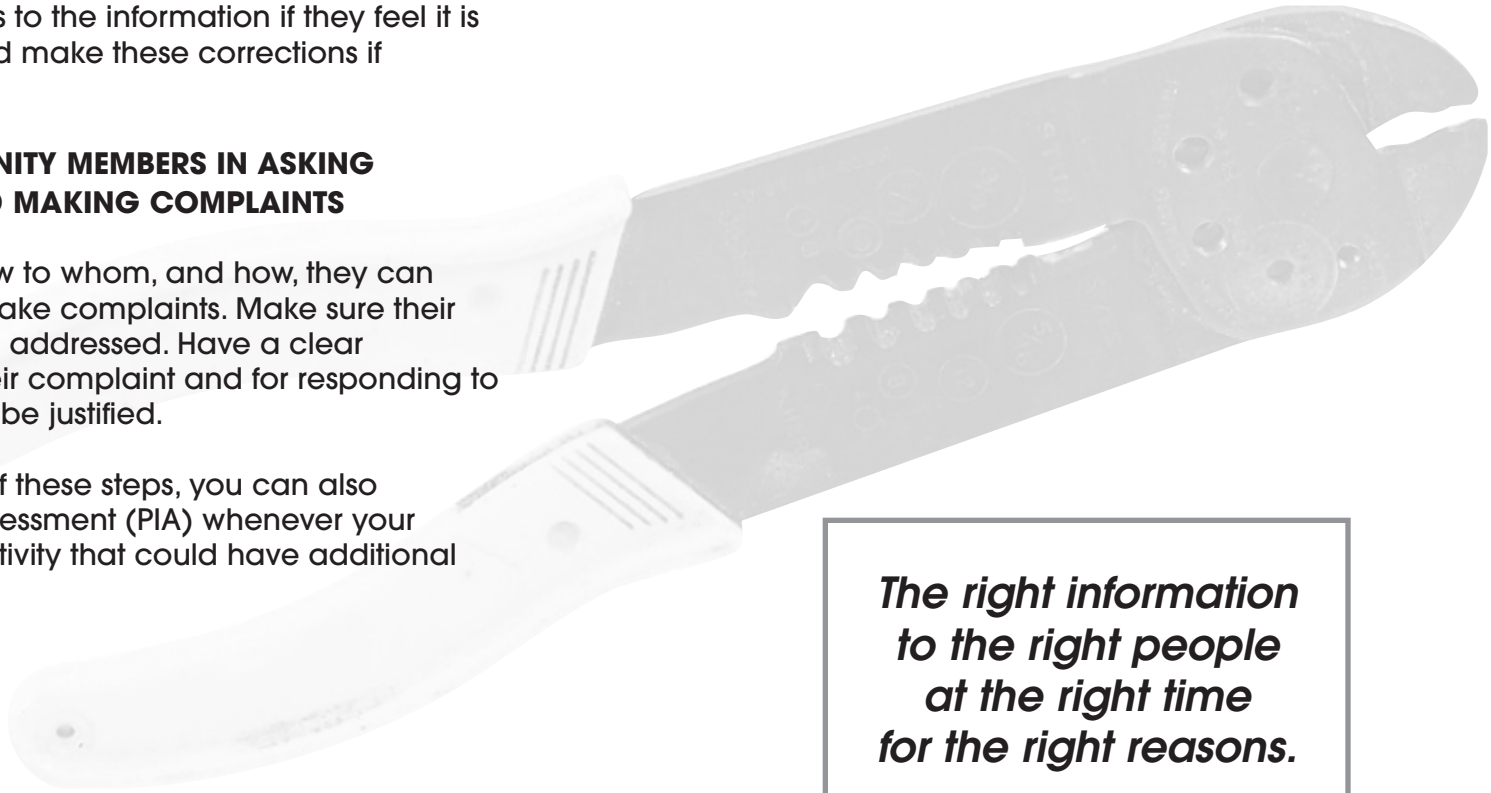
Once you have followed all of these steps, you can also conduct a Privacy Impact Assessment (PIA) whenever your community undertakes an activity that could have additional privacy risks.

A PIA is completed in three parts:

1. tracing how information flows in the course of the activity

2. determining whether the information collected, used, shared, or kept in the course of the activity is protected by laws, codes, or guidelines

3. identifying privacy risks and finding ways to reduce or eliminate these risks, such as modifying your community's guidelines or improving security measures.



The right information to the right people at the right time for the right reasons.

Ten Privacy Principles	Plan of Action for Protecting Health Information in a First Nation	Guidelines for Protecting Health Information in a First Nation
1. Accountability	**Step 1:** Identify who is responsible	**Part 1:** Who is responsible
2. Identifying Purposes	**Step 2:** Identify why information will be collected	**Part 2:** Why information is collected
3. Consent	**Step 3:** Involve community members and gain their consent	**Part 3:** Consent of community members
4. Limiting Collection	**Step 4:** Set limits on collecting information	**Part 4:** Limits on the collection of information
5. Limiting Use, Disclosure and Retention	**Step 5:** Set limits on using, sharing and safekeeping information	**Part 5:** Limits on the use, sharing and safekeeping of information
6. Accuracy	**Step 6:** Ensure that information is accurate	**Part 6:** Accuracy of information
7. Safeguards	**Step 7:** Ensure that information is secure	**Part 7:** Security measures
8. Openness	**Step 8:** Inform community members of this Plan of Action	**Part 8:** Information to community members
9. Individual Access	**Step 9:** Provide community members with access to their personal information	**Part 9:** Access of community members to their personal information
10. Challenging Compliance	**Step 10:** Assist community members in asking questions and making complaints	**Part 10:** Questions and complaints

Confidentiality: means that we keep personal information secret. Information is accessible only to those authorized to have access. It is the role of the data steward to control access to information, and to closely monitor and strictly limit access to, and disclosure of personal information.

Consent is voluntary permission from a client, or his or her legally authorized representative to collect, use, or disclose his or her own personal health information. Consent can be explicit (expressed) or implied.

- **Explicit or expressed consent** means that a client has granted formal and specific permission for the collection, use, and disclosure of his or her personal information. Explicit consent can be made in writing (such as in a form), or verbally (such as in a telephone call or personal interview).

- **Implied Consent:** Implied consent can happen in situations where the use or disclosure of the information is consistent with some purpose that the client has already agreed to, and the client understands that the information will be used for that purpose.

Data Collection: the process of gathering or obtaining personal information, or means or actions of an organization in gathering, acquiring, receiving, or obtaining personal information from any source outside the organization, including third parties, by any means.

De-identify/De-linked: in relation to the personal information of an individual, means to remove any information that,

a) identifies the individual;
b) can be manipulated by a reasonably foreseeable method to identify the individual; or
c) can be linked or matched by a reasonably foreseeable method to other information that identifies the individual, or that can be used or manipulated by a reasonably foreseeable method to identify the individual.

Disclosure: means the release, transfer, provision of access to, or divulging in any other manner of personal information outside the organization holding the information.

Informed consent can be obtained when clients are advised why the information is being collected, how the information will be used, who will have access to the information, and if their information will be disclosed to a third party. Consent must be very specific. Any overly broad statement concerning use or disclose should be avoided.

Non-identifying: when used to describe health information, means that the identity of the individual who is the subject of the information cannot be readily discovered from the information.

Personal Information: means recorded information about an identifiable individual, including:

a) the individual's name, address or telephone number;
b) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
c) the individual's age, sex, sexual orientation, marital status or family status;
d) an identifying number, symbol or other particular assigned to the individual;
e) the individual's fingerprints, blood type or inheritable characteristics;
f) information about the individual's health care history, including a physical or mental disability, or the identity of the medical practitioner consulted;
g) information about the individual's educational, financial, criminal or employment history;
h) anyone else's opinions about the individual;
i) the individual's personal views or opinions, except if they are about someone else;

or information about an identifiable individual that is recorded in any form. There are also more specific definitions of "personal

health information" contained with provincial health information privacy legislation.

Privacy: Privacy means "the right to be left alone, free from intrusion or interruption," and can include elements such as physical privacy, communications privacy, and information privacy. Privacy is linked to other fundamental human rights such as freedom and personal autonomy.

Privacy Impact Assessment (PIA): A tool used to assess the possible privacy risks of new technologies or projects. A PIA is usually required if there is significant change to information management practices in a health organization. The PIA has three components: Data Analysis Documentation (how information "flows" as a result of the project), Privacy Analysis Documentation (what are the protections in place), and a Privacy Risk Management Plan (what are the risks and how to address them).

Security: refers to procedures and tools we use to protect personal information, such as locks on doors, use of passwords for computer systems, and procedures for reporting security incidents.

Stewardship/Custodian: The data steward is a manager or trustee who has responsibility for one or more repositories/data banks of personal information. It is the steward's responsibility on a day-to-day basis to manage and control the content of the data repository, and access to the health information that it contains. Guided by a code of ethics, license and data use protocols, the data steward makes information available for a variety of purposes. The steward ensures that data are not released in a form that would violate personal or collective community privacy rights.

Third party: In relation to a request for access to a record or for correction of personal information, third party means any person, group of persons or organization other than:

a) the person who made the request; or
b) a public body (a governmental organization).

Threat Risk Assessment (TRA): a tool used to identify information assets, threats to those assets and possible security safeguards. A TRA has three major components - a Threat Analysis, a Risk Analysis, and an Assessment of Safeguards.

Sources: 1. *Guidelines for the Protection of Health Information* (COACH), 2. Discussion Paper on Ownership, Control, Access and Possession (OCAP) or Self-Determination Applied to Research, Brian Schnarch FNC@NAHO, 3. Dictionary of Key Terms Relating to Privacy for First Nations and Inuit Health Information Systems (FNIHIS), First Nations and Inuit Health Branch, Health Canada, 4. Model Code for the Protection of Personal Information, David Flaherty PhD.

Books:

Health Information Privacy (Insight Information Co., 2005)

Privacy Compliance in Healthcare (Insight Information Co., 2004)

Guide to the Ontario Personal Health Information Act (Irwin Law, 2005)

1. *Guidelines for the Protection of Health Information,* Coach Canada's Health Informatics Association, 2001.
ISBN 0-9688851-0-1

Copies:
Coach National Office
1304-2 Carleton St., Toronto, ON M5B 1J3
Tel: (416) 979-5551 or toll-free 1-888-253-8554
E-mail: Info@coachorg.com
www.coachorg.com

2. *Privacy Protection and Health Information Understanding the Implementation Issues,* March 2001. Report of the Privacy Working Group to Health Canada.

Copies:
Canadian Pharmacists Association, acting as the Privacy Working Group Secretariat
Tel: (613) 523-7877 ext. 251 or toll-free 1-800-917-9489
E-mail: gpa@cdnpharm.ca

Web Links:

ISPN Clips and Privacy News.com
www.privacynews.com

Ontario's Information Privacy Commission (Personal Health Information Protect Act)
- for guides, FAQ's and other resources
- www.ipc.on.ca

BC's Personal Information Protection website for guides, models, FAQ's and other resources:
www.mser.gov.bc.ca/privacyaccess/Privacy/

Privacy Training:

Priva-C, a division of CareLink Incorporated, specializes in information privacy and security consulting, and the development of privacy methodologies, computer-based training and other tools to help organizations implement privacy and data protection programs.

Programs and training available through Priva-C are:

- **Privacy C-Online Tutorial** - the online privacy and security awareness training has been developed by some of North America's leading privacy experts. These tutorials represent an essential first step for organizations in the implementation of privacy and security measures across their enterprises.

- **Chief Privacy Officer Workshop Training** - The Chief Privacy Officer Workshop prepares you to measure, create and maintain a successful privacy compliance system. Learn what a Chief Privacy Officer (CPO) needs to know - the key federal and provincial legislation, the policies, the difference between "security" and "privacy," how to deal with stakeholders, how to use new privacy technologies, and more.

- **Priva-C Product Suite** - offers a suite of complementary, ready-made tools that can be used independently or together for a single, seamless solution such as the Policy Generator and Gap Analysis, etc.

Contact:
Priva-C
P.O. Box 1568, Station A
Fredericton, NB E3B 5G2
Tel: (506) 450-4099 or toll-free 1-800-842-6077
Fax: (506) 459-3001
E-mail: info@priva-c.com

Privacy Experts:

Krista Yao - Expert in First Nation Privacy Issues and Legislations
Nadjiwan Law Office
Barristers & Solicitors
915 Jocko Point Road, RR4
Nipissing First Nation
North Bay, ON P1B 8G5
Tel: (705) 753-9815
Fax: (705) 753-9795
E-mail: krista@nadjiwanlaw.ca

David H. Flaherty - Specialist in Privacy and Information Policy Issues
1939 Mayfair Drive
Victoria, BC V8P 1R1
Tel: (250) 595-8897
Fax: (250) 595-8884
E-mail: David@Flaherty.com

Brendan Seaton - President and CEO of Priva-C
P.O. Box 1568, Station A
Fredericton, NB E3B 5G2
Tel: (506) 450-4099 or toll-free 1-800-842-6077
Fax: (506) 459-3001
www.brendanseaton.com

Prepared for, and reviewed by the FNIHIS Privacy Committee at its Ottawa meeting on Feb. 8, 2002, and revised on the basis of that supportive review. Presented and shared at the National Aboriginal Health Organization - Aboriginal Health Information Symposium, February 2002, Ottawa.

A Model Privacy Code for a First Nation

Revised, March 31, 2005

A Guide to Users

1. This model privacy code is based upon the principles set out in the National Standard of Canada, MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION (The CSA Model Code), CAN/CSA-Q830-96, which is also Schedule 1 to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), *Statutes of Canada,* c. 5 (2000). It must be stressed that this model code addresses personal information privacy only. It does not address OCAP concerns, as discussed earlier.

2. This code follows the 10 privacy principles, that are inherent in Canadian public sector legislation for data protection. We believe that if a First Nation is going to self-regulate, this is a general standard to work from, which can be modified to suit the needs and priorities of individual communities. The "fair information practices" in this model code are also comparable to the standards set out in federal, provincial, and territorial privacy and data protection legislation that applies to the personal information of Aboriginal Peoples held by these levels of government, and in some cases, the private and quasi-private sectors.

3. The theory behind the model code is that it will be easier for the First Nations to make progress on their privacy agendas if they have these basic principles to consider. The Carcross Tagish First Nation in the Yukon has adopted a focused privacy and access policy for census and research data that is based on the privacy laws of Ontario, British Columbia, Alberta, and the Yukon.[3] The model code presented here is a significantly more general approach to privacy and data protection for the personal information collected, used, and disclosed by Aboriginal communities.

4. The code is written for a generic First Nation or Inuit community. A specific community can simply choose to replace the generic name ("First Nation") with its own specific name. This code also calls for some kind of "independent oversight" of its implementation. The Carcross Tagish First Nation in the Yukon chose its Elders Council for that purpose.[3]

5. One advantage of using this model privacy code as a starting point for First Nation discussions is that existing literature and opinions of the Privacy Commissioner of Canada help to explain what each of these provisions means. See www.privcom.gc.ca, especially "Your Privacy Responsibilities: A Guide for Businesses and Organizations" (a booklet that can be downloaded from the World Wide Web). However, since the original drafting of this model code, privacy legislation in BC and in Ontario has come into effect. The additional privacy requirements imposed by these statutes will be noted, for the purposes of First Nations in BC and in Ontario.

6. In the absence of a statutory obligation to comply with PIPEDA or any other piece of data protection legislation, the argument is that a First Nation community may consider self-regulation for the protection of personal information on members, patients, and others that is in its custody and control.[5] Self-regulation implies exactly that; there is no legal force behind the model privacy code and no external oversight, such as by the Privacy Commissioner of Canada. In order to achieve legal force, First Nation governments (Chief and Council) would have to incorporate the privacy code into law.

7. The primary purpose of this model code would be to apply to the collection, use, and disclosure of personal information by the First Nation.

---

2 Based upon an original draft prepared by: David Flaherty, Ph.D., David H. Flaherty Inc., Privacy and Information Policy Consultants, 1939 Mayfair Drive, Victoria, BC V8P 1R1, Tel: (250) 595-8897, Fax: (250) 595-8884, email: David@Flaherty.com.

3 Carcross Tagish First Nation, "Protection of Personal Data and Information Policy," approved by Chief and Council on Sept. 30, 1998 (7 pp.). The Chief and Council are the decision-makers on access requests for personal data or information. The most extensive grounds for refusal to disclose are an unreasonable invasion of a third party's personal privacy.

4 Carcross Tagish First Nation, "Protection of Personal Data and Information Policy." A person refused access, or someone with a privacy complaint, may appeal to the Elders Council, which in effect has the authority of an Information and Privacy Commissioner.

1 Principle One - Accountability

A First Nation is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the First Nation's compliance with the following principles.

1.1

Accountability for the First Nation's compliance with the principles rests with the designated individual(s), even though other individuals within the First Nation may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the First Nation may be delegated to act on behalf of the designated individual(s).

1.2

The identity of the individual(s) designated by the First Nation to oversee its compliance with the principles shall be made known upon request.

1.3

A First Nation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The First Nation shall use contractual or other means to provide a comparable level of protection which meets any regulated requirements, and the requirements of the community.

1.4

A First Nation shall implement policies and practices to give effect to the principles, including:

a) implementing procedures to protect personal information;
b) establishing procedures to receive and respond to complaints and inquiries;
c) training staff and communicating to staff information about the First Nation's policies and practices; and
d) developing information to explain the First Nation's policies and procedures.

2 Principle Two - Identifying Purposes

The First Nation, at or before the time information is collected, shall identify the purposes for which personal information is collected.

2.1

The First Nation shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 8) and the Individual Access principle (Clause 9).

2.2

Identifying the purposes for which personal information is collected, at or before the time of collection, allows a First Nation to determine the information it needs to collect to fulfill these purposes. The Limiting Collection principle (Clause 4) requires a First Nation to collect only that information necessary for the purposes that have been identified.

2.3

The identified purposes should be specified, at or before the time of collection, to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless law permits the new purpose, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 3).

2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

2.6

This principle is linked closely to the Limiting Collection principle (Clause 4) and the Limiting Use, Disclosure, and Retention principle (Clause 5).

3 Principle Three - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate or where permitted or required by statute.

Note: In certain circumstances, personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law

5 Aboriginal communities collect and use personal information on their members with respect to membership, housing, loans, education, health, and social support services (for example).

enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. When in doubt about whether consent is required, a First Nation shall consult professional advice.

3.1

Except where permitted by law, consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, a First Nation will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when a First Nation wants to use information for a purpose not previously identified).

3.2

The principle requires "knowledge and consent." A First Nation shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used, and to whom it may be disclosed. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

3.3

A First Nation shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes.

3.4

The form of the consent sought by the First Nation may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, a First Nation shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context.

3.5

In obtaining consent, the reasonable expectations of the individual are also relevant.

3.6

The way in which a First Nation seeks consent may vary, depending on the circumstances and the type of information collected. A First Nation should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. An authorized representative (such as a legal guardian or a person having power of attorney) can also give consent.

3.7

Individuals can give consent in many ways. For example:

a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
b) a check-off box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
c) consent may be given orally when information is collected over the telephone; or
d) consent may be given at the time that individuals use a product or service. Ontario privacy legislation defines specific circumstances when implied consent can be relied upon, and when express consent is mandatory.

3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions, and reasonable notice. The First Nation shall inform the individual of the implications of such withdrawal.

4 Principle Four - Limiting Collection

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

4.1

A First Nation shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. A First Nation shall specify the type of information collected as part of its information-handling policies and practices, in accordance with the Openness principle (Clause 8).

4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent the collection of personal information by misleading or deceiving individuals about the purpose for which information is being collected.

5 Principle Five - Limiting Use, Disclosure, and Retention

information shall not be used or disclosed for purposes other than those for which it was collected, except with consent or as required or permitted by law.

5.1

A First Nation using personal information for a new purpose shall document this purpose (see Clause 2.1) and the steps taken to obtain consent.

5.2

A First Nation should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made.

5.3

Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. A First Nation shall develop guidelines and implement procedures to govern the destruction of personal information, with reference to any minimum retention periods required by law or regulations.

5.4

Sensitive community information shall not be used or disclosed for purposes other than those for which the First Nation has consented to, or as required by law. The First Nation will develop policies and procedures for the First Nation, where appropriate, to enter into information sharing agreements with third parties to protect the privacy of sensitive community information.

6 Principle Six - Accuracy

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

6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

6.2

A First Nation shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

7 Principle Seven - Safeguards

Security safeguards appropriate to the sensitivity of the information shall protect personal information.

7.1

Security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. A First Nation shall protect personal information regardless of the format in which it is held.

7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. A higher level of protection should safeguard more sensitive information. The concept of sensitivity is discussed in Clause 3.

7.3

The methods of protection should include:

a) physical measures - for example, locked filing cabinets and restricted access to offices;
b) organizational measures - for example, security clearances and limiting access on a “need-to-know” basis; and
c) technological measures - for example, the use of passwords and encryption.

7.4

A First Nation shall make its employees aware of the importance of maintaining the confidentiality of personal information, and shall have employees swear or affirm a confidentiality oath.

7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 5.3).

8 Principle Eight - Openness

A First Nation shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

8.1

A First Nation shall be open about its policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about a First Nation's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

8.2

The information made available shall include:

a) the name or title, and the address, of the person who is accountable for the First Nation's policies and practices and to whom complaints or inquiries can be forwarded;
b) the means of gaining access to personal information held by the First Nation;
c) a description of the type of personal information held by the First Nation, including a general account of its use;
d) a copy of any brochures or other information that explain the First Nation's policies, standards, or codes; and
e) what personal information is made available to related organizations (e.g. subsidiaries).

8.3

A First Nation may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, a First Nation may choose to make brochures available in its place of business, mail information to its clients, or provide online access.

9 Principle Nine - Individual Access

Upon request, and subject to limits permitted by law, 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 request a correction.

Note: In certain situations, a First Nation may not be able to provide access to all the personal information it holds about an individual. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide; information that contains references to other individuals; information that cannot be disclosed for legal, security, or commercial proprietary reasons; information that is subject to solicitor-client or litigation privilege, or information that may harm the health or well-being of the client or someone else.

9.1

Upon request, a First Nation shall inform an individual whether or not the First Nation holds personal information about the individual. A First Nation is encouraged to indicate the source of this information. The First Nation shall allow the individual access to this information. However, the First Nation may choose to make sensitive medical information available through a medical practitioner. In addition, the First Nation shall provide an account of the use that has been made, or is being made of this information, and an account of the third parties to which it has been disclosed.

9.2

An individual may be required to provide sufficient information to permit a First Nation to provide an account of the existence, use, and disclosure of personal information. The information provided shall be used only for this purpose.

9.3

In providing an account of third parties to which it has disclosed personal information about an individual, a First Nation should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the First Nation shall provide a list of organizations to which it may have disclosed information about the individual.

9.4

A First Nation shall respond to an individual's request within a reasonable time, and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the First Nation uses abbreviations or codes to record information, an explanation shall be provided.

9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the First Nation shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

Continued from p.18

9.6

When a challenge is not resolved to the satisfaction of the individual, the First Nation shall record the substance of the unresolved challenge. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

10 Principle Ten - 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 First Nation's compliance.

10.1

The individual accountable for a First Nation's compliance is discussed in Clause 1.1.

10.2

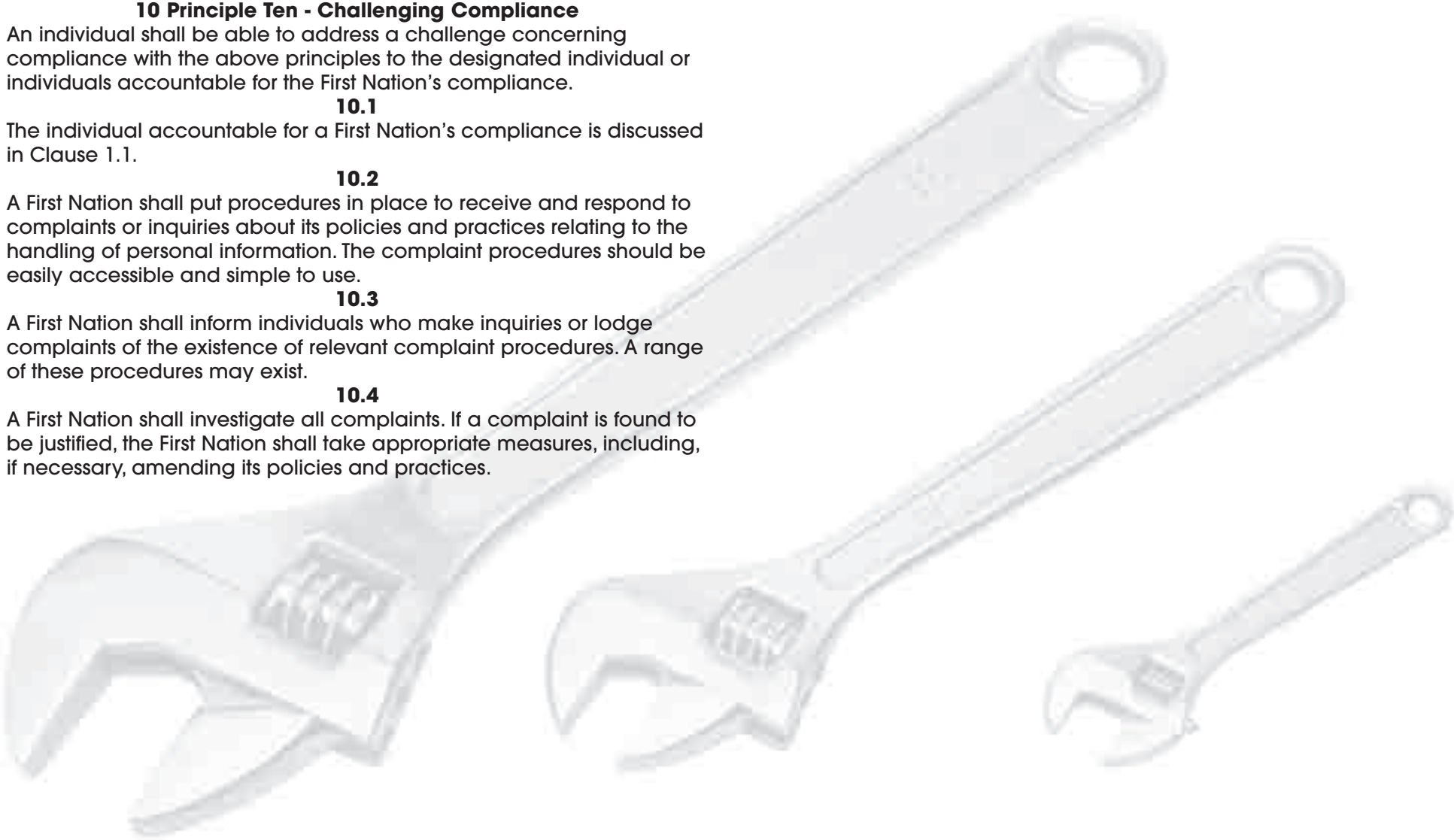
A First Nation shall put procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

10.3

A First Nation shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist.

10.4

A First Nation shall investigate all complaints. If a complaint is found to be justified, the First Nation shall take appropriate measures, including, if necessary, amending its policies and practices.



Continued from p.19

First Nations Centre des Premières Nations
FNC PN
©NAHO ONSA

220 Laurier Avenue West, Suite 1200
Ottawa, ON K1P 5Z9
Tel: (613) 237-9462
Fax: (613) 237-1810
Toll-free: 1-877-602-4445
Email: fnc@naho.ca
Website: www.naho.ca/fnc

National Aboriginal Health Organization (NAHO)
Organisation nationale de la santé autochtone (ONSA)
ᑳᓇᑕᒥ ᓄᓇᖃᖅᑳᖅᓯᒪᔪᐃᑦ ᖃᓄᐃᙱᓯᐊᓚᓱᐊᖅᓂᒧᑦ ᑎᒥᖁᑎᖓᑦ