

Consultation Draft: May 2005



Consultation Draft: May 2005

DISCLAIMER	
<p>This Privacy Code Document has been prepared by CaNIOS for its membership, for the ownership and use of the CaNIOS members, as a general guide to assist each CaNIOS member and centre to meet their obligations under the <i>Personal Information Protection and Electronic Documents Act</i> (PIPEDA) Canada, 2000 and the <i>Personal Health Information Protection Act</i> (PHIPA). Ontario, 2004.</p>	
1.	This Executive Summary of Privacy and Confidentiality is designed to provide information to assist in complying with the law and meeting the changing expectations of patients and the public.
2.	The material provided in this Executive Summary of Privacy and Confidentiality is for general information purposes only. It should be adapted to the circumstances of each institution or physician using the CaNIOS National Registry.
3.	The Executive Summary of Privacy and Confidentiality reflects interpretations and practices regarded as valid when it was published based on available information at that time.
4.	The Executive Summary of Privacy and Confidentiality is not intended, and should not be construed, as legal or professional advice or opinion.
5.	CaNIOS centres and members concerned about the applicability of privacy legislation to their activities are advised to seek legal or professional advice based on their particular circumstances.
6.	In addition, Ontario's Information and Privacy Commissioner has an important role to play in providing further guidance on how the Personal Health Information Protection Act, 2004 is being applied and interpreted. Websites to monitor are: http://www.ipc.on.ca http://www.health.gov.on.ca/english/public/updates/archives/hu_03/priv_legislation.html
7.	This is the first version of the CaNIOS Executive Summary of Privacy and Confidentiality. A second version may be released in due course. Your feedback on this first edition would be appreciated.
8.	This first version of the CaNIOS Executive Summary of Privacy and Confidentiality is compliant with the Ontario Privacy Law. Future versions will be released in due course meeting the requirements of other provincial privacy laws.

Consultation Draft: May 2005

Executive Summary

The Canadian Network for Improved Outcomes in SLE (CaNIOS) is an independent, national, not-for-profit organization. The following pages provide an overview of CaNIOS' mandate, as agreed upon by its members on February 14, 2002.

Mission Statement:

“A group of Canadian investigators coming together to improve the outcome of lupus patients across our country through collaborative research.”

Goals:

1. To facilitate the care of Canadian lupus patients.
2. To improve the outcomes in Canadian lupus patients.
3. To describe the lupus patient population in Canada.
4. To facilitate research in lupus and related autoimmune diseases.
5. To provide a large patient base to address clinically important issues through research.
6. To take advantage of the unique features in the Canadian lupus population.
7. To look at sub-groups of the Canadian lupus population: the pediatric lupus patients, minorities, and men.
8. To contribute to the global and international effort on lupus research through the uniqueness of the Canadian lupus population.
9. To provide mentorship to young investigators and trainees who are interested in developing a career in lupus research.

The core values of the CaNIOS National Registry are:

- 1) Respect for the privacy of the health information of the persons enrolled into the Registry.
- 2) Respect for the privacy / sanctity of the SLE cohorts of the CaNIOS centres.
- 3) Recognition of the research value of the CaNIOS collaborative National Registry.

The challenge is to balance these values in a way that maximizes the benefits of all three values, while minimizing the potential harms from neglecting any of them. In order to achieve a good balance, assessment must be done to ensure that the potential benefits of the research to the public outweighs the potential harm to the research participants of the CaNIOS National Registry.. Also to be taken into account is the degree of risk associated with the sensitivity of the collected data: all data must be stored in highly-secured environments, with physical, technological and administrative protections in place in order to ensure the integrity of the data, the privacy of the individual, and the sanctity of the individual CaNIOS centres cohorts.

The following are examples of how the core values listed above reflect the context within which the CaNIOS National Registry operates:

Consultation Draft: May 2005

- The CaNIOS National Registry receives personal health information from SLE cohort databases of CaNIOS centres that have the authority to disclose the information to CaNIOS for the purpose of carrying out its mandate. CaNIOS relies on these organizations to comply with the privacy requirements and laws in place in their jurisdictions for the collection, use and disclosure of personal health information;
- The CaNIOS National Registry receives, on an annual basis, coded personal health information that represents a fraction of the information in the original records of the individuals concerned;
- The CaNIOS National Registry records include a unique identifier to facilitate statistical analysis and research. This number is usually the cohort number assigned to the individual at his/her treating centre. The key linking the unique number to the individual does not reside at the CaNIOS National Registry but rather with the individual's own personal lupus specialist. Thus the data the CaNIOS National Registry receives are not readily identifiable of an individual. Nonetheless, the CaNIOS National Registry protects the data to the same degree as readily identifiable personal information;

CaNIOS uses health information for analysis and reporting to improve the health of the Canadian lupus population and to transform the health care system. Given its mandate, CaNIOS does not use the personal health information to make health care decisions for the individual study participant.

- CaNIOS supports access to de-identified personal health information in a responsible, secure manner for purposes of analysis and research, consistent with CaNIOS' mandate.

Consultation Draft: May 2005

Introduction

The principles articulated in this document are based on the ten principles found in the Code for the Protection of Personal Information, Can/CSA-Q830-96, which is now Schedule 1 to the *Personal Information Protection and Electronic Documents Act*, (PIPEDA) statutes of Canada, 2000, c.6.

These principles are:

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limited use, disclosure, and retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

CaNIOS uses personal health information for the following purposes:

- To conduct research that contributes to the effectiveness, quality, equity, and efficiency of health care for the SLE population of Canada;
- To carry out health services research in areas of clinical and policy relevance from a population- and disease-based perspective;
- To document “Canada-wide” patterns of the “natural” history of SLE on an ongoing basis;
- To develop and disseminate information and decision tools for use by SLE patients, families and friends, practitioners, clinician-managers, administrators, and policymakers;
- To implement and evaluate projects in a clinical setting so as to promote more effective and efficient patterns of care;
- To promote collaboration among lupus researchers and health service researchers in Canada, and between researchers and decision-makers;
- To train lupus researchers and health service researchers in order to promote a wider understanding of relevant concepts regarding the clinical epidemiology of SLE and related autoimmune diseases.

Consultation Draft: May, 2005

PRINCIPLES

Principle 1 – Accountability

Principles and procedures for ensuring confidentiality and security of data are strictly enforced to respect the privacy of users and the stewardship of the providers of the CaNIOS National Registry; as well as, to protect data against loss, destruction or unauthorized use. The CaNIOS National Registry is responsible for all data held in its possession or custody.

CaNIOS' Executive Chair and the Chair of the Data Access Subcommittee and designates are responsible for the CaNIOS National Registry compliance and adherence to the principles outlined in this document. They are also accountable for ensuring that all research studies are implemented in accordance with the current standards for ethical acceptability, and that they adhere to the principles of privacy, confidentiality and security found in the CaNIOS Privacy Code.

Principle 2 – Identifying Purposes

The primary purpose of the collection and use of personal health information by CaNIOS scientists is to describe the lupus patient population in Canada, and to provide a large patient base to address clinically important issues through research.

CaNIOS will identify additional purposes for which its scientists use personal health information by developing research proposals and study designs/plans *before* information is used (administrative, registry, survey databases) or collected (primary clinical data collection or chart review). Data is used for research and statistical purposes only.

Principle 3 – Consent

The burden of obtaining consent is on the individual CaNIOS investigator supplying personal health information to the CaNIOS National Registry, since the Registry Manager and each CaNIOS investigator does not have a direct relationship with all the individuals on whom it holds data.

Individuals can give consent in three different ways.

(A) A CaNIOS cohort participant may sign a study-specific customized consent form, outlining the purpose of the study, the information to be collected, the risks and benefits of study participation, and a description of the use that will be made of the information.

(B) A CaNIOS cohort participant may provide explicit consent to the transfer of their personal health information obtained in the context of the 'annual' cohort

Consultation Draft: May, 2005

visit and other specific studies, to third party researchers such as the CaNIOS National Registry databank.

- (C) A CaNIOS cohort participant may verbally provide consent to the transfer of their personal health information to the CaNIOS National Registry when appropriate to the study methodology.

The consent principle requires “knowledge and consent”. CaNIOS personnel will advise an individual of the clinical research purposes for which their information will be used. To make the consent meaningful, the purposes will be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. The consent will also articulate the possibility of sharing the data with other researchers in a de-identified form for future projects. If record linkages are to be carried out on the collected data, the individual will be informed in advance which additional data stored at CaNIOS will be used to augment the research project. Specific consent for these linkages will be sought at the time the original consent is signed.

Principle 4 – Limiting Collection

CaNIOS will limit amount and type of personal information collected to that which is necessary to fulfill the research purposes of the Network or research studies.

Principle 5 – Limit Use, Disclosure, and Retention

All individual cohort registry data received into the CaNIOS National Registry will be used only for research and statistical purposes. All primary data will be used only for the purposes identified prior to the collection of the data.

CaNIOS *does not disclose* individual-level information which it uses or collects under any circumstances. Such an act would contravene its research agreements and this Code.

The CaNIOS National Registry presents data in an *anonymized* and *aggregate* fashion: ie. data is “collective” and grouped together to be used in research.

Personal information collected in the context of clinical trials and epidemiological studies will not be used for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

Personal information is retained and securely archived at the individual CaNIOS centres as is required for clinical research projects for a maximum period of twenty-five (25) years. In project-specific research agreements, earlier or later destruction may be a requirement. CaNIOS has provided for its centres policies and procedures pertaining to the disposal and destruction of personal information to prevent unauthorized parties from gaining access to information.

Consultation Draft: May, 2005

Principle 6 – Accuracy

Individual cohort registry data that has been made anonymous cannot be updated, unless the individual CaNIOS centre collecting the data verifies and updates the information.

Personal information collected for clinical trials and epidemiological studies will be as accurate, complete and up-to-date as possible at the time of the collection.

Principle 7 – Safeguards

CaNIOS will protect all data within its custody and all data is considered to be highly sensitive. Information protection is paramount and accomplished with overlapping security safeguards.

The nature of the safeguards will vary depending on the individual CaNIOS centres' location; the amount, distribution, and format of the information; and, the methods of protection available.

The methods of protection at each CaNIOS centre include:

- (a) **Physical measures:** e.g., locked facility with tracked key access, locked filing cabinets and restricted access to offices, internal/external video monitoring of the institute;
- (b) **Organizational measures:** e.g., strict employee confidentiality agreements (with immediate dismissal as a sanction) and limiting access on a “need-to-use” basis;
- (c) **Technological measures:** e.g., two-stage firewall (device & software), secured socket layer encryption user/id password authentication (capability for fingerprint ID), intruder detection, passwords; and
- (d) **Anonymization** of data by stripping conventional identifiers

The methods of protection of the CaNIOS National Registry situated at the SoftWorks office include:

- (a) **Physical measures:** e.g., secure hosting facility, 24-hr surveillance, keypad entry & auditing, bullet-proof encasement around the machine room, access limited by changing security locks, appropriate attention to flooding and fire threat;
- (b) **Organizational measures:** e.g., strict employee confidentiality agreements (with immediate dismissal as a sanction) and limiting access on a “need-to-use” basis;
- (c) **Technological measures:** e.g., secure (https;) access to the internet, actively maintained firewalls, ongoing virus/worm surveillance, “moating” of data (making it inaccessible externally), passwords, encryption of data, regular backup and restore procedures; and,
- (d) **Anonymization** of data by stripping conventional identifiers, “private – public key encryption” process: random scrambling of identifiers with an algorithm.

Consultation Draft: May, 2005

As a condition of access to the CaNIOS National Registry, CaNIOS requires that all personnel, including CaNIOS scientists, adjunct scientists, fellows and students, sign a confidentiality agreement upon becoming a member of CaNIOS. This agreement is reviewed and re-signed each time there is a change in the CaNIOS Chair. On an ongoing basis, CaNIOS makes its membership aware of the importance of maintaining the confidentiality of personal information.

Principle 8 – Openness

CaNIOS will make information about its policies and practices related to the management and protection of personal information readily available in both printed form and on the corporate web site – (www.canios.ca). This information will be made available in a form that is generally understandable.

Principle 9 – Individual access

The CaNIOS National Registry cannot provide access to anonymized personal information held within the individual centres' registry datasets. Upon request from an individual, CaNIOS will inform the individual's centre of the general data sources CaNIOS uses for research and statistical purposes, and will refer the individual to the primary collector of such data (ie: a patient of Dr John Hanly's for the Halifax Lupus Cohort).

Upon request, (*see form appendix 1*) an individual participating in a clinical study or survey will be informed of the use of his/her personal information and may be given access to that personal information by the CaNIOS investigator associated with the study. The individual will be given a duplicate copy of his/her signed consent form, outlining the study plan and principles.

Principle 10 – Challenging compliance

An individual will be able to address a challenge concerning compliance with the above principles directly to the designated individuals whom are accountable for CaNIOS' compliance. These individuals will generally include the Chair of CaNIOS, the Chair of the Privacy Compliance subcommittee, and designates.