Standards

COLLEGE & ASSOCIATION OF REGISTERED NURSES OF ALBERTA

Expert caring makes a difference®

Privacy and Management of Health Information

Standards for CARNA's Regulated Members

September 2011

Approved by the College and Association of Registered Nurses of Alberta (CARNA) Provincial Council, September 2011.

College and Association of Registered Nurses of Alberta
11620 – 168 Street
Edmonton, AB T5M 4A6

Phone: 780.451.0043 (in Edmonton) or 1.800.252.9392 (Canada-wide)
Fax: 780.452.3276
Email: practice@nurses.ab.ca
Website: www.nurses.ab.ca

Table of Contents

Preamble

On September 1, 2010 amendments to Alberta's *Health Information Act* (HIA) came into force. Until the most recent amendments, the Act only applied to health services paid for under the Alberta Health Care Insurance Plan. Under the amended Act, the Act applies to all health information collected, used and disclosed, **by custodians**, in relation to a health service regardless of how it is paid for. "Health information" and "health services" have specific, defined meanings under the Act.

The associated HIA Regulation designates who are custodians under the Act. Regulated members of specific health professions have been designated as custodians. The HIA amendments will apply to regulated members[1] of the College and Association of Registered Nurses of Alberta (CARNA) on September 1, 2011.

All regulated members of CARNA will be custodians for the purposes of the HIA unless they are an affiliate of another custodian. Individuals who are affiliates of another custodian are deemed not to be a custodian while acting in the capacity of an affiliate. **An "affiliate" is:**

- **an individual employed by a custodian**
- **a person who performs a service for a custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian**
- **a health services provider who is exercising the right to admit and treat patients at a hospital as defined in the *Hospitals Act***

Examples of custodians include:

- Alberta Health Services
- Covenant Health
- nursing home operators

Therefore, registered nurses employed by these organizations are affiliates.

[1] Regulated members of CARNA are: registered nurses (RN), graduate nurses (GN), nurse practitioners (NP), graduate nurse practitioners (GNP), and certified graduate nurses (CGN).

Regulated members of CARNA may also be self-employed or employed by other organizations such as private industry, corporations and educational institutions that are not custodians under HIA. These organizations may employ regulated members of CARNA who provide health services. Although the employer is not a custodian under the HIA, the regulated member is subject to HIA for the health information that they collect for the purpose of providing a health service (for example, health information about employees of the organization). **Any regulated member of CARNA practising in an employment setting where they collect health information for the purpose of providing a health service is a custodian under HIA.** An example of this is an occupational health nurse who is employed by a large oil company to provide health services to the organization's employees.

It is important to remember that the HIA does not apply to health information that is collected for purposes other than providing health services. Further, the HIA Regulation excludes a number of services from the definition of health services. For example, insurance companies may hold health information in their files but they are not custodians, as the HIA does not govern the use of health information by them. Two other examples include: the review, interpretation or assessment of results from a drug or alcohol test to determine an individual's fitness to work; and the review, interpretation or assessment of results from medical or health monitoring of an individual to protect the health of workers or determine the individual's fitness to work. (See Appendix A).

Regulated members of CARNA must continue to be aware of and follow all relevant privacy legislation. Regulated members will still be governed by a variety of privacy legislation that applies to the personal information that they collect, use and disclose. Where the *Health Information Act* does not apply, Alberta's *Personal Information Protection Act* (PIPA) or the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) may.

Regulated members recognize the importance of privacy and confidentiality. The ethical obligations of registered nurses with respect to maintaining privacy and confidentiality are embodied in the *Code of Ethics for Registered Nurses*, as incorporated into the *Nursing Practice Standards*.

The *Nursing Practice Standards* apply to overall care and to all regulated members of CARNA in clinical practice, research, education and administration. This document builds on those standards and identifies standards for maintaining privacy and confidentiality as well as the management of information in records and the management of electronic records, including the protection, privacy and security of electronic records.

For the purposes of the standards set out below, "health information" refers to health information collected, used or disclosed in relation to a health service, as defined in the *Health Information Act*.

CARNA Standards for Privacy and Management of Health Information

1. The regulated member is personally responsible and accountable for ensuring that they understand the privacy requirements that apply to their practice.

2. The regulated member collects, uses, and discloses only the amount of health information that is essential for the intended purpose and with the highest degree of anonymity possible.

3. The regulated member takes reasonable steps to ensure the accuracy of health information before using or disclosing the information.

4. The regulated member accesses personal and health information, including electronic health records, only for purposes that are consistent with their professional responsibilities.

5. The regulated member intervenes or takes action if others inappropriately access or disclose personal or health information of persons receiving care.

6. The regulated member is personally responsible and accountable for identifying and confirming whether they are a custodian of health information or an affiliate of a custodian for the purposes of health information legislation and shall advise the College of their status, when requested.

7. The regulated member who is a custodian is personally responsible and accountable for identifying the health information that they collect for the purposes of providing a health service. This will assist the regulated member in identifying and complying with legislated requirements specific to health information.

8. The regulated member who is an affiliate of a custodian of health information is personally responsible and accountable for ensuring that they are familiar with and comply with the legislated requirements specific to health information as well as their custodian's policies and procedures regarding the collection, use, disclosure and security of personal and health information.

9. The regulated member who is a custodian of health information is personally responsible and accountable for ensuring that they and their affiliates are familiar with and comply with the legislated requirements specific to health information.

10. The regulated member who is a custodian must take reasonable steps to ensure that client records are accessible for continuity of care for clients. Client records must remain accessible for a period of ten (10) years following the date of last service. For minors, the record must be accessible for a period of ten (10) years or two (2) years past the patient's age of majority, whichever is longer.

11. The regulated member who is a custodian of health information establishes written policies and procedures relating to how they and their affiliates handle health information in their custody and control. These policies and procedures necessarily include a written record of the administrative, technical and physical safeguards in place to protect the privacy and confidentiality of health information in their custody and control. These must include:

- affiliates are only given access to health information needed for their role
- reasonable measures to physically secure the areas in which health information is stored such as locked buildings or rooms, locked filing cabinets, and locked shredding bins
- reasonable measures to maintain the security of health information while it is being transported from one location to another
- reasonable measures for the secure disposal of records containing health information

12. In additional to Standard 11, the regulated member who is a custodian of health information who uses a computerized or electronic information system must ensure that the system has reasonable safeguards to protect the confidentiality and security of the information, including but not limited to, ensuring that:

a. each authorized user can be uniquely identified

b. each authorized user has a documented access level based on the user's role

c. access to the system is password protected with procedures for password management and updates

d. the system creates and maintains audit logs that meet legislative requirements for electronic health record information systems

e. identifiable health information is transmitted securely

f. appropriate anti-virus systems, firewalls and intrusion detection systems are installed and monitored

g. data is backed up securely

h. data recovery protocols are in place and regularly tested

i. protocols are in place to ensure continuity of care in the event that the information contained within the electronic information system cannot be accessed for a period of time

j. secure disposal of hardware that contains identifiable health information such that all data is removed and cannot be reconstructed

13. The regulated member who is a custodian ensures that their affiliates are aware of and adhere to all of their policies and procedures regarding the collection, use, disclosure and security of personal and health information and establishes sanctions for any breach thereof.

14. The regulated member who is a custodian who collects health information for the purposes of providing a health service who is employed by a non-custodian must:

a. inform the employer of the regulated member's obligations as a custodian

b. review the employer's policies and procedures relating to the collection, use, disclosure, retention and security of health information

c. make recommendations to the employer regarding the collection, use, disclosure, retention and security of health information to ensure that legislated requirements specific to health information and their obligations as custodians are met and reflected in the employer's policies and procedures

d. where the custodian uses the employer's electronic information systems for health information, the custodian shall use reasonable efforts to enter into a written agreement with their employer that addresses their respective obligations regarding the collection, use, disclosure, retention and security of health information

15. The regulated member who is a custodian of health information periodically assesses the administrative, technical and physical safeguards in respect of:

- the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information
- any reasonably anticipated threat or hazard to the security or integrity of the health information or to the loss of the health information
- any unauthorized use, disclosure or modification of the health information or unauthorized access to the health information

16. The regulated member who is a custodian must comply with all legislative requirements, including:

a. the preparation and submission of a Privacy Impact Assessment to the Privacy Commissioner, before implementing any proposed new practice or system relating to the collection, use and disclosure of individually identifying health information

b. providing clients with access to their personal and health information in compliance with access to information legislation and subject to any statutory exceptions and fees, and allowing for the correction of personal and health information, as required by law

17. If a regulated member who is a custodian places health information in an electronic information management system that is not under their direct custody and control, there must be in place a written agreement that addresses the security of the health information, responding to access to information requests, and the collection, use and disclosure of the health information by the person or body who has custody or control of the health information through the electronic system, as well as any other requirements for such an agreement as set out at law.

18. The regulated member must comply with any written direction by CARNA to make specific health information accessible via the Alberta electronic health record.

References

Alta. Reg. 118/2010. [*Alberta Electronic Health Record Regulation*].

Alta. Reg. 70/2001. [*Health Information Regulation*].

Canadian Nurses Association. (2008). *Code of ethics for registered nurses*. Ottawa, ON: Author.

College and Association of Registered Nurses of Alberta. (2003). *Nursing practice standards*. Edmonton, AB: Author.

Health Information Act, R.S.A. 2000, c. H-5.

Personal Information Protection Act, S.A. 2003, c. P-6.5.

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Resources

Alberta Government – Service Alberta. www.servicealberta.ca/pipa

Office of the Information and Privacy Commissioner of Alberta. www.oipc.ab.ca

Office of the Information and Privacy Commissioner of Alberta. (2010). *Health information: A personal matter: A practical guide to the Health Information Act*. Edmonton, AB: Author.

Office of the Privacy Commissioner of Canada. www.priv.gc.ca

Appendix A

ALBERTA REGULATION 70/2001

Health Information Act

HEALTH INFORMATION REGULATION

Exclusion from definition of health service

3.1 For the purposes of section 1(1)(m) of the Act, the following services are excluded from the definition of health service:

(a) the review, interpretation or assessment by a health services provider of

(i) results from a drug or alcohol test performed on a bodily substance from an individual, but only to the extent necessary or reasonably required to determine the individual's fitness to work,

(ii) results

(A) from medical, health or biological monitoring of an individual, or

(B) from medical or health surveillance of an individual, but only to the extent necessary or reasonably required to protect the health of workers or to determine the individual's fitness to work, or

(iii) results from a medical or health assessment of an individual, but only to the extent necessary or reasonably required to determine the individual's fitness to work;

(b) the review, interpretation or assessment of health information about workers collected under the *Occupational Health and Safety Act* by the Director of Medical Services for the purposes of protecting the health and safety of workers;

(c) an independent medical examination of an individual, or a review of the health information of an individual, by a health services provider who is not involved in the treatment and care of the individual for the purpose of determining benefits or coverage, or both, for insurance purposes;

(d) services, including parenting psychological assessments, neuro-psychological assessments and individual or group counselling, provided by psychologists to

children and families at the request of a director under the *Child, Youth and Family Enhancement Act*;

(e) the review, interpretation or assessment by a health services provider of results from a drug or alcohol test performed by a laboratory on a bodily substance from an individual at the request of a director under the Child, Youth and *Family Enhancement Act*;

(f) emergency response dispatch services.