College of Registered Nurses of Alberta

nurses.ab.ca

Privacy and Management of Health Information Standards

December 2022

Effective March 31, 2023

Approved by the College of Registered Nurses of Alberta (CRNA) Council, December 2022, effective March 31, 2023.

The College and Association of Registered Nurses of Alberta (CARNA) is operating as the College of Registered Nurses of Alberta (CRNA).

College of Registered Nurses of Alberta
11120 – 178 Street
Edmonton, AB T5S 1P2

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

Table of Contents

Purpose

These standards are developed and approved as outlined in Section 133 of the *Health Professions Act* (2000). These standards apply to **REGISTRANTS**[1] of the CRNA at all times, in every domain of practice.

The purpose of these standards is to

- outline the responsibilities of registrants when managing **HEALTH INFORMATION**; and
- outline the Health Information Act (HIA, 2000) requirements for **CUSTODIANS** and **AFFILIATES** of health information.

Background

The HIA (2000), the *Health Information Regulation* (Alta Reg 70/2001), and the *Alberta Electronic Health Record Regulation* (Alta Reg 118/2010) outline expectations for the collection, use, disclosure, and security of health information that protects the privacy and confidentiality of individuals and their health information. The HIA balances the protection of privacy with sharing health information to provide a **HEALTH SERVICE** and manage the health system. Regardless of how a health service is paid for, the HIA applies to all health information collected, used, and disclosed by custodians in relation to that health service.

Registrants are governed by a variety of privacy legislation, which applies to the personal information that they collect, use, and disclose. Where the HIA (2000) does not apply, Alberta's *Personal Information Protection Act* (PIPA, 2003), *Freedom of Information and Protection of Privacy Act* (FOIP, 2000), or the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA, 2000) may. Registrants are accountable for understanding which legislation applies to their nursing practice.

The HIA (2000) does not apply to health information collected for purposes other than to provide health services. The *Health Information Regulation* (Alta Reg 70/2001) excludes a number of services from the definition of health services (Appendix A).

[1] Words or phrases displayed in **BOLD CAPITALS** upon first mention are defined in the glossary.

Custodians and Affiliates

Custodians are the gatekeepers of the health information and can include registrants. Registrants are custodians for the purposes of the HIA unless they are an affiliate of another custodian.

Custodians

The HIA (2000) identifies custodians as

- hospital boards, nursing home operators, provincial health boards;
- ambulance operators, regional health authority, the Health Quality Council of Alberta, licensed pharmacies; and
- health-care professionals that are designated under the *Health Information Regulation* (Alta Reg 70/2001).

Registrants may be self-employed or employed to provide health services by other organizations such as private industry or clinics, corporations, and educational institutions, which are not custodians under the HIA (2000). When registrants practicing in these settings collect health information for the purpose of providing a health service, then they are the custodians under the HIA.

Examples of this are occupational health nurses employed by a large oil company to provide health services to the organization's employees, or occupational health nurses at a post-secondary educational institution. In these cases, the registrant is the custodian, as these employers have not been identified as a custodian under the HIA (2000).

In compliance with the *Health Information Act* (2000) and regulations, the CRNA has created the *Privacy and Security Policies for Custodians: Information and Templates* (2023). This document provides a template for the development of policies and procedures registrants, as custodians, can use when submitting a **PRIVACY IMPACT ASSESSMENT** (PIA) to the Office of the Information and Privacy Commissioner (OIPC).

Affiliates

Registrants are affiliates of health information if they practice in an organization identified as a custodian. The HIA (2000) describes "affiliate" as follows:

- an individual or organization 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 **CLIENTS** at a hospital, as defined in legislation

Duty to Report a Privacy Breach

The HIA (2000) amendments came into force on August 31, 2018 and mandates:

> *"a custodian must as soon as practicable give notice in accordance with the regulations... of any loss of... or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure"*

(HIA, 2000, s 60.1[2]).

The process to report a breach, including who reports the breach, will vary according to employer requirements. To comply with mandatory reporting of a privacy breach, registrants who are custodians of health information must

- assess the risk of harm to an individual when their health information has been lost or inappropriately accessed or disclosed;
- report to the privacy commissioner *(www.oipc.ab.ca*), minister of health (*www.alberta.ca/health.aspx*), and the individual who was subject to the loss, unauthorized access, or disclosure of their health information; and
- report to the privacy commissioner when and why there has been a determination to not report a privacy breach to an individual.

Section 107 of the HIA (2000) clearly identifies the offences and penalties for contravention of the requirements of the Act. A person found guilty of one of these offences is subject to fines up to $50,000.

Standards for Privacy and Management of Health Information

Custodians of health information must ensure they follow the same responsibilities as affiliates, and have additional roles and responsibilities as custodians. All registrants must ensure they understand all responsibilities with respect to privacy and management of health information, as affiliates or as custodians.

These standards for privacy and management of health information, identify the minimum expectations of CRNA registrants. The criteria describe how registrants must meet each standard and are not listed in order of importance.

Standard 1: All Registrants

Registrants are responsible and accountable for ensuring they follow all relevant privacy legislation and policies, and understand the privacy requirements that apply to their nursing practice.

Criteria

All registrants must

1.1 access personal and health information, including electronic health records (EHR), only for purposes that are consistent with their professional responsibilities;

1.2 collect, use, and disclose only health information that is essential for the intended purpose, with the highest degree of confidentiality possible, and in accordance with legislation;

1.3 know their custodian's requirements regarding collection, use, disclosure, and security of health information;

1.4 take reasonable steps to ensure the accuracy of health information before using or disclosing the information;

1.5 comply with any written direction by the CRNA to make specific health information accessible via the *Alberta Electronic Health Record Regulation* (Alta Reg 118/2010);

1.6 notify the custodian (if the registrant is an affiliate) as soon as practicable of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying information, in the custody or control of the custodian; and

1.7 report any inappropriate access or disclosure of personal or health information of persons receiving care.

Standard 2: Registrants as Custodians

In addition to the above standard, registrants as custodians of health information are responsible for the safeguarding of health information according to all relevant legislation.

Criteria

Registrants as custodians must

2.1 submit evidence of their status as custodian to the CRNA or any other applicable authority if or when requested;

2.2 report any inappropriate access or disclosure of personal or health information of persons receiving care as per legislation and employer requirements;

2.3 comply with all legislative requirements, including

- **a)** preparing and submitting a PIA to the privacy commissioner before implementing any proposed new or changing 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,
- **c)** performing a risk of harm assessment in the event of a privacy breach of an individual as a result of the loss of, unauthorized access to, or disclosure of individually identifying health information that considers all relevant factors,
- **d)** giving notice to the privacy commissioner, the minister of health, and the individual when the risk of harm assessment confirms risk to the individual due to loss of health information or any unauthorized access to or disclosure of individually identifying health information, and
- **e)** notifying the privacy commissioner immediately of the decision not to give notice to an individual who is the subject of a privacy breach, in the event it could be **REASONABLY** expected to result in a risk of harm to the individual's mental or physical health;

2.4 be responsible and accountable for identifying information they collect for the purposes of providing a health service as health information;

2.5 be responsible and accountable for ensuring that they and their affiliates are familiar with, and comply with, the legislated requirements specific to health information;

2.6 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 client's age of majority, whichever is longer;

2.7 establish written policies and procedures relating to how they and their affiliates handle health information and submit these policies and procedures when requested. Policies and procedures 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

- **a)** limiting affiliates' access to health information needed for their role,
- **b)** 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,
- **c)** reasonable measures to maintain the security of health information while it is being transported from one location to another,
- **d)** reasonable measures for the secure disposal of records containing health information, and
- **e)** direction on how information will be transferred from one custodian to another;

2.8 ensure that, when using a computerized or electronic information system, the system has reasonable safeguards to protect the confidentiality and security of the information, including but not limited to

- **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 creating and maintaining audit logs that meet legislative requirements for electronic health record information systems, as set out in the *Alberta Electronic Health Record Regulation* (Alta Reg 118/2010),
- **e)** identifiable health information is transmitted securely,
- **f)** appropriate antivirus 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, and

j) disposal of hardware that contains identifiable health information is secure and complete, such that all data is removed and cannot be reconstructed;

2.9 regularly assess the administrative, technical, and physical safeguards with respect to

a) the confidentiality of health information that is in their custody or under their control, and the privacy of the individuals who are the subjects of that information,

b) any reasonably anticipated threat or hazard to the security or integrity of the health information, and

c) any unauthorized use, access to, disclosure, or modification of the health information;

2.10 ensure that, when placing health information in an electronic information management system that is not under their direct custody and control, they

a) establish a written agreement that addresses the security of the health information,

b) establish the protocol for responding to access to information requests, and the collection, use, and disclosure of health information by the person or body who has custody or control of the health information through the electronic system, and

c) establish any other requirements for such an agreement as set out in law.

Registrants as custodians of health information, and employed by a non-custodian, must also

2.11 clearly communicate their obligations of a custodian to the employer;

2.12 review the employer's requirements relating to the collection, use, disclosure, retention, and security of health information and ensure requirements align with legislation; and

2.13 collaborate with employers to ensure that legislated requirements specific to health information, and their obligations as custodians are met and reflected in the employer's requirements and procedures regarding the collection, use, disclosure, retention, and security of health information.

Glossary

Affiliate – Means "affiliate" as defined in the HIA (RSA 2000 cH-5). An affiliate includes the following:

- an individual or organization 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 clients at a hospital, as defined in legislation

Client – The term client(s) can refer to patients, residents, families, groups, communities and populations.

Custodian – Means "custodian" as defined in the HIA (2000). A custodian includes the following:

- hospital boards, nursing home operators, provincial health boards
- ambulance operators, regional health authority, the Health Quality Council of Alberta, licensed pharmacies
- health-care professionals that are designated under the *Health Information Regulation* (Alta Reg 70/2001).

Health information – Means "health information" as defined in the HIA (2000) and refers to health information collected, used, or disclosed in relation to a health service.

Health service – "Means a service that is provided to an individual for any of the following purposes:

i. protecting, promoting or maintaining physical and mental health;

ii. preventing illness;

iii. diagnosing and treating illness;

iv. rehabilitation;

v. caring for the health needs of the ill, disabled, injured or dying,

but does not include a service excluded by the regulations."

(HIA, 2000, s.1[1][m])

Privacy impact assessment – An analysis of processes performed by a custodian that assists in identification of and addressing potential privacy risks that may occur in the collection, use or disclosure of individually identifying personal or health information (Office of the Information and Privacy Commissioner of Alberta, n.d.).

Reasonably – Enough credible evidence to lead an ordinary person to prudent judgment of the suspicions and belief that individual holds.

Registrant(s) – Includes registered nurses (RNs), graduate nurses, certified graduate nurses, nurse practitioners (NPs), graduate nurse practitioners, and RN or NP courtesy registrants on the CRNA registry.

References

Alberta Electronic Health Record Regulation, Alta Reg 118/2010.

College of Registered Nurses of Alberta. (2023). *Privacy and security policies for custodians: Information and templates*.

Freedom of Information and Protection of Privacy Act, RSA 2000, c F-25.

Health Information Act, RSA 2000, c H-5.

Health Information Regulation, Alta Reg 70/2001.

Health Professions Act, RSA 2000, c H-7.

Office of the Information and Privacy Commissioner of Alberta. (n.d.). *Privacy impact assessments*. Retrieved July 8, 2022, from *https://oipc.ab.ca/privacy-impact-assessments/*.

Personal Information Protection Act, SA 2003, c P-6.5.

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

Appendix A: Exclusion from Definition of Health Service

Health Information Regulation **(Alta Reg 70/2001)**

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.