CRNA College of Registered Nurses of Alberta

nurses.ab.ca

# Privacy and Management of Health Information Standards

March 2020

11120 178 Street, Edmonton, AB, T5S 1P2 1 (800) 252-9392 crna@nurses.ab.ca

Approved by the College and Association of Registered Nurses of Alberta (CARNA) Council, March 2020.

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



Ensure you are using the current version of this document by visiting our website.

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

The purpose of these standards is to:

- outline the responsibilities of regulated members[1] when managing health information; and
- outline the *Health Information Act* (HIA) (2000) requirements for **CUSTODIANS**[2] and **AFFILIATES** of **HEALTH INFORMATION.**

These standards apply to regulated members at all times, in every domain of practice.

# Background

The HIA, the *Health Information Regulation* (2001), and the *Alberta Electronic Health Record Regulation* (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.

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

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

[1] The term "regulated members" includes all CARNA regulated members such as registered nurses, graduate nurses, certified graduate nurses, nurse practitioners, graduate nurse practitioners, and RN or NP courtesy regulated members.
[2] Words or phrases 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 regulated members. Regulated members are custodians for the purposes of the HIA unless they are an affiliate of another custodian.

## Custodians

The HIA identifies custodians as:

- hospital boards, nursing home operators, provincial health boards;
- health-care providers providing health services; and
- health-care professionals that are designated under the *Health Information Regulation* (2001).

Regulated members 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. When regulated members practicing in these settings collect health information for the purpose of providing a health service, then they are the custodians under the HIA.

An example of this is 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 regulated member is the custodian, as these employers have not been identified as a custodian under the HIA.

In compliance with the *Alberta Electronic Health Record Regulation* (2010), CARNA has created the *Privacy and Security Policies for Custodians: Information and Templates* (2020). This document provides a template for the development of policies and procedures regulated members as custodians can use when submitting a **Privacy Impact Assessment** (PIA) to the Office of the Information and Privacy Commissioner (OIPC).

## Affiliates

Regulated members are affiliates of health information if they practice in an organization identified as a custodian. The HIA 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 service provider who is exercising the right to admit and treat **clients** at a hospital, as defined in the *Hospitals Act* (2000)

# Duty to Report a Privacy Breach

The HIA 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).

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, regulated members 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 (*oipc.ab.ca*), Minister of Health (*alberta.ca/health-information-act.aspx*), and the individual who was subject to the improper use, 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 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

Regulated members as custodians have additional roles and responsibilities as affiliates. However, all regulated members must ensure they understand all responsibilities with respect to privacy and management of health information, as affiliates or as custodians.

## Standard 1: All Regulated Members

Regulated members 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.

**All regulated members 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 policies and procedures 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 CARNA to make specific health information accessible via the *Alberta Electronic Health Record Regulation* (2010);

**1.6** notify the custodian (if the regulated member 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: Regulated Members as Custodians

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

**Regulated members as custodians must**

**2.1** submit evidence of their status as custodian to CARNA 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 policy;

**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 (Appendix B),
- **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 (Appendix C), 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 (Appendix D);

**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 *Electronic Health Records Regulation* (2010),
- **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, 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.

**Regulated members 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 policies and procedures relating to the collection use, disclosure, retention, and security of health information and ensure policy aligns 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** – According to the HIA (2019), an affiliate includes the following:

- employees of a custodian
- any person that performs a service for a custodian (agent, appointee, volunteer or student)
- health-care providers who can admit/treat patients at hospitals and other health- care practitioners with formal access to hospital resources

**Client** – The term client(s) can refer to patients, residents, families, groups, communities, and population (CARNA, 2013).

**Custodians** – According to the HIA (2019), a custodian includes the following:

- hospital boards, nursing home operators, provincial health boards, etc.
- health-care providers that provide health services
- licensed pharmacy and/or pharmacists
- health-care professionals that are designated under the *Health Information Regulation* (2001)

**Health information** – Refers to health information collected, used, or disclosed in relation to a health service (HIA, 2000).

**Health service** – A service provided to people to protect, promote, or maintain their health; to prevent illness; diagnose; treat; rehabilitate; or to take care of the health needs of the ill, disabled, injured or dying (HPA, 2000).

**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 health information (Office of the Information and Privacy Commissioner of Alberta, 2019).

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

# References

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

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

Canadian Health Services Research Foundation. (2005). How CHSRF defines evidence. *Links*, *8*(3), 7.

Canadian Nurses Association. (2010). *Canadian nurse practitioner core competency framework*. Retrieved from http://cna-aiic.ca/~/media/cna/files/en/competency_framework_2010_e.pdf.

Canadian Nurses Association. (2017). *Code of ethics for registered nurses*. Ottawa, ON: Author.

College and Association of Registered Nurses of Alberta. (2013). *Practice standards for regulated members*. Edmonton, AB: Author.

College and Association of Registered Nurses of Alberta. (2020). *Privacy and security policies for custodians: Information and templates*. Edmonton, AB: Author.

*Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25.

Government of Alberta. (2019). *Alberta Netcare Learning Centre: Health Information Act*. Retrieved from *http://www.albertanetcare.ca/LearningCentre/Health-Information-Act.htm.*

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

*Health Profession Act*, R.S.A. 2000, c. H-7.

*Hospitals Act*, R.S.A. 2000, c. H-12.

Office of the Information and Privacy Commissioner of Alberta. (2019). *Privacy impact assessments*. Retrieved from *https://www.oipc.ab.ca/action-items/privacy-impact-assessments.aspx*.

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

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

# Appendix A: Exclusion from Definition of Health Service

**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.

# Appendix B: Assessment of Risk of Harm

**ALBERTA REGULATION 70/2001**

**Health Information Act**

**HEALTH INFORMATION REGULATION**

**Assessment of risk of harm**

**8.1(1)** In assessing under section 60.1(4) of the Act whether there is a risk of harm to an individual as a result of a loss of or an unauthorized access to or disclosure of individually identifying health information, a custodian must consider each of the following factors in addition to any other relevant factors:

- **a.** whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;
- **b.** whether there is a reasonable basis to believe that the information has been misused or will be misused;
- **c.** whether there is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud;
- **d.** whether there is a reasonable basis to believe that the information is of a type that could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual who is the subject of the information;
- **e.** whether there is a reasonable basis to believe that the loss of or unauthorized access to or disclosure of the information has adversely affected or will adversely affect the provision of a health service to the individual who is the subject of the information;
- **f.** in the case of electronic information, whether the custodian is able to demonstrate that the information was encrypted or otherwise secured in a manner that would
    - **i.** prevent the information from being accessed by a person who is not authorized to access the information, or
    - **ii.** render the information unintelligible by a person who is not authorized to access the information;

**g.** in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was

**i.** destroyed, or

**ii.** rendered inaccessible or unintelligible;

**h.** in the case of a loss of information that is subsequently recovered by the custodian, whether the custodian can demonstrate that the information was not accessed before it was recovered;

**i.** in the case of an unauthorized access to or disclosure of information, whether the custodian is able to demonstrate that the only person who accessed the information or to whom the information was disclosed was

**i.** is a custodian or an affiliate,

**ii.** is subject to confidentiality policies and procedures that meet the requirements of section 60 of the Act,

**iii.** accessed the information in a manner that is in accordance with the person's duties as a custodian or affiliate and not for an improper purpose, and

**iv.** did not use or disclose the information except in determining that the information was accessed by or disclosed to the person in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure.

**(2)** If a custodian is able to demonstrate that a circumstance set out in subsection (1)(f) to (i) applies in the case of a loss of or unauthorized access to or disclosure of individually identifying health information, the custodian is not required to give notice of the loss or unauthorized access or disclosure under section 60.1(2) of the Act.

# Appendix C: Notice of Loss or Unauthorized Access or Disclosure

**ALBERTA REGULATION 70/2001**

**Health Information Act**

**HEALTH INFORMATION REGULATION**

**Notice of loss or unauthorized access or disclosure**

**8.2(1)** A notice to a custodian under section 60.1(1) of the Act must

- **a.** if the custodian has established requirements respecting the notice, meet any requirements respecting form and contents established by the custodian, or
- **b.** if the custodian has not established requirements respecting the notice, be in writing and include
  - **i.** a description of the circumstances of the loss or unauthorized access or disclosure,
  - **ii.** the date on which or period of time within which the loss or unauthorized access or disclosure occurred,
  - **iii.** the date on which the loss or unauthorized access or disclosure was discovered, and
  - **iv.** a description of the information that was lost or that was the subject of the unauthorized access or disclosure.

**(2)** A notice to the Commissioner of a loss of or an unauthorized access to or disclosure of individually identifying health information under section 60.1(2) of the Act must be in writing in a form approved by the Commissioner and must include

- **a.** the name of the custodian who had custody or control of the information at the time of the loss or unauthorized access of disclosure,
- **b.** a description of the circumstances of the loss or unauthorized access or disclosure,
- **c.** the date on which or period of time within which the loss or unauthorized access or disclosure occurred,

**d.** the date on which the loss or unauthorized access or disclosure was discovered,

**e.** a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure,

**f.** a non-identifying description of the risk of harm to an individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed that includes a non-identifying description of the custodian's consideration of the factors referred to in section 8.1(1), including any relevant factors not detailed in that section,

**g.** the number, or if the number cannot be determined, an estimate of the number, of individuals to whom there is a risk of harm as a result of the loss or unauthorized access or disclosure,

**h.** a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of harm to an individual as a result of the loss or unauthorized access or disclosure,

**i.** a description of any steps that the custodian has taken or is intending to take as of the date of the notice, to reduce the risk of a future loss or unauthorized access or disclosure,

**j.** a non-identifying copy of the information that has been or will be provided in the notice to the individual who is the subject of the individually identifying health information referred to in subsection (4), if applicable, together with a statement indicating the method referred to in section 103 of the Act that has been or will be used to give notice to the individual, if applicable,

**k.** if the custodian is requesting the authorization of the Commissioner to give notice to an individual by substitutional service under section 103(c) of the Act, the request together with a statement of the reasons for the request,

**l.** the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure, and

**m.** any other information that the custodian considers relevant.

**(3)** A notice to the Minister of a loss of or an unauthorized access to or disclosure of individually identifying health information under section 60.1(2) of the Act must be in writing in a form approved by the Minister and must include the information set out in subsection (2)(a), (b), (e), (f), (g), (h), (l) and (m).

**(4)** A notice to an individual of a loss of or unauthorized access to or disclosure of individually identifying health information under section 60.1(2) of the Act must be in writing and must include

**a.** a description of the circumstances of the loss or unauthorized access of disclosure,

**b.** the date on which or period of time within which the loss or unauthorized access or disclosure occurred,

**c.** the name of the custodian who had custody or control of the health information at the time of the loss or unauthorized access or disclosure,

**d.** a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure,

**e.** a description of the risk of harm to the individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed,

**f.** a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of harm to the individual as a result of the loss or unauthorized access or disclosure,

**g.** a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of a future loss or unauthorized access or disclosure,

**h.** a description of any steps that the custodian believes the individual may be able to take to reduce the risk of harm to the individual,

**i.** a statement that the individual may ask the Commissioner to investigate the loss or unauthorized access or disclosure that includes contact information for the Office of the information and Privacy Commissioner,

**j.** the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure, and

**k.** any other information that the custodian considers relevant.

# Appendix D: Notice to Commissioner of Decisions not to Give Notice

**ALBERTA REGULATION 70/2001**

**Health Information Act**

**HEALTH INFORMATION REGULATION**

**Notice to Commissioner of decision not to give notice**

**8.3** A notice to the Commissioner under section 60.1(5) of the Act of a decision not to give notice to an individual must

- **a.** be in writing in a form approved by the Commissioner,
- **b.** have attached as an appendix the notice required to be provided to the Commissioner in respect of the matter under section 60.1(2) of the Act, and
- **c.** set out the total number, or if the number cannot be determined, an estimate of the total number, of individuals that the custodian expects not to give notice to on the basis set out in section 60.1(5) of the Act.