CARNA College & Association of Registered Nurses of Alberta

Privacy and Security Policies
A Guide for Custodians

September 2013

Privacy and Security Policies A Guide for Custodians

Table of Contents

Purpose 3

Policy Description 4
1. Roles and Responsibility 4
2. Right of Access 5
3. Information Handling and Security 9
4. Collection, Use and Disclosure of Health Information 13
5. Information Privacy and Security in Contracting 18
6. Research 20
7. Transitory Records 21
8. Alberta Electronic Health Record (Alberta Netcare) 22
9. Penalties/Sanctions 23
10. Distribution 24
11. Approval 25

Appendix 1: HIA Definitions 26
Appendix 2: Privacy and Management of Health Information Standards for CARNA's Regulated Members 28
Appendix 3: Request to Access Health Information and/or Pharmacy Access Log 29
Appendix 4: Refusal by Custodian to make Correction or Amendment 31
Appendix 5: Request to Correct or Amend Health Information 33
Appendix 6: Components for an Affiliate's Oath of Confidentiality 35
Appendix 7: Sample Mini-poster 37
Appendix 8: Section 41 Notation 38
Appendix 9: Section 42 Notification 39
Appendix 10: Consent to the Disclosure of Health Information 40

Purpose

These policies and procedures were developed in order to meet the legislative requirements set out by the *Health Information Act* (HIA). The associated HIA Regulation designates who are custodians under the Act and regulated members[1] of CARNA are designated as custodians.

The Office of the Information and Privacy Commissioner was asked by CARNA to review this guide and OIPC indicated that the guide provides a good template that will assist CARNA's membership with establishing policies and procedures that will facilitate their compliance with section 63 of HIA. HIA definitions are included in Appendix 1.

A custodian of health information must establish **written** policies and procedures relating to how they and their affiliates handle health information in their custody and control. These policies and procedures need to include a written record of the administrative, technical and physical safeguards in place to protect the privacy and confidentiality of health information.

This guide provides information and templates that can be used by you, as a custodian of health information, when developing policies and procedures for use in your practice setting and when completing a Privacy Impact Assessment (PIA) submission to the Office of the Information and Privacy Commissioner. These same policies and procedures can also be used when submitting a PIA for a request to access Alberta Netcare.

You will need to individualize and adapt the policy and procedures in this guide to reflect your own specific organizational privacy management procedures so that you can use them as part of your PIA submission to the Office of the Information and Privacy Commissioner. If you have any questions about your role as a custodian, please contact a CARNA Policy and Practice Consultant at practice@nurses.ab.ca

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

Policy 1
Roles and Responsibilities

Role and Responsibility of Privacy Officer

1.1 The individual in the practice setting who will be the Privacy Officer for HIA matters must be identified.

1.2 If the privacy officer in the setting is away, then who will act as Privacy Officer until such time as the other returns must be indicated.

1.3 Responsibilities of the Privacy Officer include:

i. Identifying privacy compliance issues in the practice setting.

ii. Ensuring that all privacy policies and security procedures are developed and maintained.

iii. Ensuring that all staff, students, volunteers, and contracted personnel are aware of their duties, roles, and responsibilities under applicable privacy legislation.

iv. Providing advice regarding the disclosure and non-disclosure of health information.

v. Responding to requests for access to health information.

vi. Ensuring proper retention and disposal of health information.

vii. Acting as a contact when dealing with the Office of the Information and Privacy Commissioner.

Responsibilities of all staff (custodians and affiliates) include:

1.4 Protecting the confidentiality of any health information they may have access to through the performance of their job responsibilities.

1.5 Collecting, using, and disclosing health information only in the performance of their job responsibilities.

1.6 Reading and signing-off that they have read and understood the privacy policies and security procedures for the collection, use and disclosure of health information.

1.7 Reporting privacy breaches to the Privacy Officer in the practice setting.

1.8 All CARNA regulated members must adhere to the *Privacy and Management of Health Information: Standards for CARNA's Regulated Members* (Appendix 2).

Policy 2

Right of Access to Health Information

Informal Requests

2.1 A request from a client to access or to correct or amend their own personal basic health information is handled informally. If uncertain of client identity then valid identification must be presented (e.g. driver's license, Alberta Health Care Insurance Plan Card). For example the request to correct or amend basic health information could be to change address or contact information.

Formal Requests

2.2 Request to Access to health information

A request for access to health information which cannot be handled informally must be made in writing (see Appendix 3). A request for access to health information in Netcare must be in writing. A custodian is responsible to respond to a formal request to access health information whether in a point of care information system or Netcare.

A person may request access to another individual's information only if they have:

i. that individual's written authorization, or

ii. proof of being that individual's authorized representative

A response to an applicant's written request must be made within 30 days of receipt of the request.

An individual may request a copy of an audit log showing who has accessed their health information.

2.3 Request to Correct or Amend information

A request to correct or amend information which cannot be handled informally must be made in writing (see Appendix 5). A request to correct or amend information in Netcare must be in writing. A custodian is responsible to respond to a formal request to correct information whether in a point of care information system or Netcare.

An applicant may request a correction/amendment to another individual's information only if he or she has proof of being that individual's authorized representative as set out under section 104 of HIA.

Procedure to request correction or amendment to information

i. The Privacy Officer, custodian, as well as appropriate staff members will determine whether the request is to be granted or refused. Custodians are not obliged to make changes based on opinions; however they must consider the request and make a decision based on their professional judgment. The correction process must be completed within 30 days of receipt of the request for correction, unless the time has been extended in accordance with HIA.

ii. In the case of a correction/amendment or refusal thereof, the Privacy Officer shall ensure that the correction/amendment has or has not been made and inform the applicant of the same in writing (see Appendix 4 for refusal letter).

iii. The Privacy Officer will advise any person to whom the information was disclosed in the preceding year that a correction or amendment was made. The only exception being where:

    a. The custodian believes the applicant will not be harmed if notification is not provided; and the applicant agrees.

iv. If the request is refused and the applicant elects to submit a statement of disagreement as outlined on the form, the statement shall be attached (if reasonably practical) to the information that is the subject of the request for correction or amendment. Any person to whom the record has been disclosed in the year preceding the date of the request shall receive a copy of the statement of disagreement.

2.4 Non-Disclosure (in relation to an access request)

Mandatory exceptions to disclosure: Health information must not be disclosed to an applicant:

i. If it is about an individual other than the applicant, unless it was originally provided by the applicant in the context of a health service for the applicant (i.e. the applicant provided his/her family medical history to the regulated member of CARNA. For example, the applicant's record contains the statement, "My father has a history of heart disease."),

ii. If it sets out procedures or contains results of an investigation, discipline proceeding, practice review or an inspection related to a health services provider or,

iii. If the disclosure is prohibited by legislation.

Discretionary exceptions to disclosure: Health information may not be disclosed to the applicant if the disclosure could reasonably be expected to:

i. Result in immediate and grave harm to the applicant's mental or physical health or safety,

ii. Threaten the health or safety of another individual or the public,

iii. Pose a threat to public safety,

iv. Lead to the identification of a person who provided health information in confidence or

v. Be expected to prejudice the use or results of audits, diagnostic tests or assessments.

2.5 If health information is partly disclosed, the excepted information will be removed (severed) from the record prior to the record being disclosed to the applicant. The applicant will be advised that information was severed and under what sections of the HIA the exceptions were made. The applicant will be provided with a contact name in the practice setting who can answer questions about the severing decisions.

2.6 The applicant will be informed they can ask the Office of Information and Privacy Commissioner (OIPC) for a review of granting/refusing access decisions and granting/ refusing correction requests.

2.7 If the applicant views the original record, a staff member shall be present to answer questions and maintain the integrity of the record.

Authorized Representatives

2.8 As set out under s.104 of HIA, the following persons may exercise any right, including an individual's right to correct or amend their health information:

i. if the individual is 18 years of age or older, by the individual,

ii. if the individual is under 18 years of age and understands the nature of the right or power and the consequences of exercising the right or power, by the individual,

iii. if the individual is under 18 years of age but does not understand the nature of the right or power and the consequences of exercising the right or power, by the guardian of the individual

iv. if the individual is deceased, by the individual's personal representative (e.g. administrator or executor) if the exercise of the right or power relates to the administration of the individual's estate,

v. if a guardian or trustee has been appointed for the individual under the *Adult Guardianship and Trusteeship Act*, by the guardian or trustee if the exercise of the right or power relates to the powers and duties of the guardian or trustee,

vi. if an agent has been designated under a personal directive under the *Personal Directives Act*, by the agent if the directive so authorizes,

vii. if a power of attorney has been granted by the individual, by the attorney if the exercise of the right or power relates to the powers and duties conferred by the power of attorney,

viii. by the individual's nearest relative as defined in the *Mental Health Act* if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act, or

ix. by any person with written authorization from the individual to act on the individual's behalf.

2.9 When an authorized representative as set out above seeks to access or correct/amend health information, it is the applicant's responsibility to provide documentation to demonstrate he/she is the individual's Authorized Representative.

2.10 Staff will carefully review documentation provided by the applicant to ensure they have authority to act on behalf of the individual and, where appropriate, will keep a copy of such documentation.

2.11 Every reasonable effort to assist the applicant and to respond openly, accurately and completely shall be made. This includes providing an explanation of any term, code or abbreviation used in the record.

Policy 3

Information Handling and Security

Administrative Safeguards

If a custodian wishes to use the services of an information manager (HIA s. 66(1)) HIA requires that the custodian enter into a written agreement (HIA s. 66(2)) with an information manager in accordance with section 7.2 of the *Health Information Regulation.*

3.1 Information privacy and security policies and procedures have been developed and are updated as necessary based on the results of a regular review (e.g. yearly).

3.2 Only the least amount of information necessary for the intended purpose is collected, used and disclosed.

3.3 Access to health information is restricted to staff who require access to the health information in order to perform their job duties.

3.4 Confidentiality and security of health information is addressed as part of the conditions of employment for new staff and is written into job description and contracts.

3.5 Staff is monitored for compliance with privacy policies and security procedures.

3.6 All new staff is required to review privacy policies and security procedures, and sign off that they have read, understood and will abide by them.

3.7 All staff are required to attend privacy and security, training sessions

3.8 All staff, students, volunteers and contracted personnel (e.g. janitors, temporary staff, etc.) are required to sign an Oath of Confidentiality (see Appendix 6).

3.9 The following process is to be adhered to by any employees, staff, students, volunteers or contracted personnel who cease to practice, work or volunteer in the setting or their employment has been terminated:

i. all sensitive materials are to be retrieved including access control items like badges, keys, fobs or security tokens, and revocation of door and access keys and cards;

ii. all system related documentation is to be retrieved;

iii. all user accounts, passwords and alarm codes are to be terminated.

3.10 Health information is not shared verbally if conversations can be overheard or intercepted.

3.11 A Privacy Impact Assessment (PIA) is to be completed and submitted to the Office of the Information and Privacy Commissioner before implementing a new or making a change to an existing administrative practice or information system that is used for the collection, use and disclosure of individually identifying health information,.

3.12 All privacy compliance issues and security breaches are reported to the Privacy Officer in the setting.

3.13 Health information is retained in accordance with specific records retention provisions as set out by CARNA in the document *Privacy and Management of Health Information: Standards for CARNA's Regulated Members*.

Technical Safeguards

3.14 All electronic information system users are assigned a unique identifier (user ID) that restricts access to health information and systems that are required for the administration of their job responsibilities.

3.15 Access to electronic systems is password protected.

3.16 Passwords are kept confidential at all times and are not to be written down, posted publicly or shared with other staff. As a best practice it is preferred that passwords be at least 8 characters long, and include at least one number and one symbol (e.g. @#$%^&).

3.17 Passwords are changed every 3 months.

3.18 Screen saver passwords are used to protect against unauthorized access if a computer is left unattended.

3.19 Health information sent via email over public or external networks is encrypted.

3.20 Information systems must be capable of creating and maintaining logs of access to patient information. The log should contain the following information:

i. user identification associated with an access
ii. role or job function of user
iii. date and time of an access
iv. actions performed by the user (e.g. creating, viewing, editing, deleting)
v. identification of the individual whose record was accessed (e.g. name, personal health number)

3.21 Information systems are audited to detect unauthorized access and prevent modification or misuse of health information.

3.22 Audit trails are reviewed as deemed necessary by the custodian, and on an incident basis.

3.23 Health information is protected from unauthorized external access by a firewall.

3.24 Virus scanning software is installed to protect health information from unauthorized modification, loss, access or disclosure.

3.25 Systems are regularly patched with critical patches being applied as soon as possible. Automatic update should be enabled for operating systems.

3.26 Electronic systems are backed up on a daily basis.

3.27 Back-up information is stored in a secure, locked environment off-site.

3.28 Information intended for long term storage on electronic media (e.g. tape, DVD, disk) is reviewed on an annual basis to ensure the data is retrievable and to migrate the data to another storage medium if necessary.

3.29 Installing or Altering Software. The custodian is responsible for authorizing and approving all software installations and alterations. Installed software is periodically reviewed and unneeded software is removed from the system.

Physical Safeguards

3.30 Records, both on-site and off-site, are held and stored in an organized, safe and secure manner.

3.31 Rooms and/or cabinets used to store health information are locked when not in use.

3.32 Records storage areas are equipped with smoke detectors, fire extinguishers and sprinkler systems when possible.

3.33 The distribution of keys is strictly controlled.

3.34 Building premises are protected by building alarms. Alarm codes are changed as deemed necessary by the custodian.

3.35 Health information is not left unattended in areas to which the public has access.

3.36 Computer monitors are positioned so that on-screen information cannot be viewed by others.

3.37 Any electronic system's network server is located in a locked area.

3.38 Individuals are prevented from viewing health information unless looking directly at the screen.

3.39 When health information is transported to another location, it is placed in a sealed envelope, marked as confidential and directed to the attention of the authorized recipient.

3.40 Staff verify the identity of courier services used for the transportation of health information.

3.41 Fax machines are located in a secure area.

3.42 Pre-programmed numbers are not used to send fax transmissions of identifiable health information.

3.43 All fax transmissions are sent with a cover sheet that indicates the information being sent is confidential and requesting that the information be returned to the practice setting if sent to the wrong number.

3.44 Reasonable steps are taken to confirm that health information transmitted via fax is sent to a secure fax machine and to confirm that the information was received.

3.45 Health information in paper format is disposed of by confidential shredding.

3.46 Destruction is documented by listing the records/files to be destroyed, recording the date of destruction and having an employee/staff member sign off that the destruction occurred.

3.47 All hardware that contains health information is securely disposed of so that all data is removed and cannot be reconstructed.

Security breaches

3.48 All security breaches or privacy compliance issues are reported to the Privacy Officer in the practice setting.

3.49 The Privacy Officer will investigate the breach and evaluate the severity based on the degree of harm to the individuals involved, the sensitivity of the information, and the degree of intent. Additional staff will be involved in the investigation as necessary to determine the cause of the breach and to implement any corrective or disciplinary actions required.

3.50 Depending on the nature and severity of the breach, the Privacy Officer will notify the Office of the Information and Privacy Commissioner that a breach has occurred.

3.51 The results of the investigation will be communicated to appropriate staff and corrective action will be taken.

3.52 Any applicable sanctions will be applied by the appropriate supervisory staff.

Policy 4

Collection, Use and Disclosure of Health Information

Collection of Health Information

4.1 An individual's health information is collected directly from the individual who is the subject of the information, or his/her Authorized Representative, unless:

i. the individual consents to the indirect collection of the information;

ii. collection would compromise the interests of the individual, the purpose of collection, the accuracy of the information or the safety of any other person;

iii. direct collection is not reasonably practicable;

iv. the information is collected for the purpose of compiling a family or genetic history in order to provide a health service to the individual;

v. the information is collected to assess the individual's ability to participate in a program, or receive a benefit, product or health service;

vi. the information is collected to inform the Public Trustee or Public Guardian about clients or potential clients;

vii. the information is publicly available; or

viii. the information is disclosed in accordance with Part 5 of HIA (the disclosure rules).

4.2 A poster is displayed in the practice setting to inform clients of the purpose and authority for the collection of information, and the availability of the Privacy Officer to answer questions or concerns (see Appendix 7).

Use of Health Information

4.3 Health information is only used for the following purposes (referred to as Authorized Uses):

i. to provide health services,

ii. to determine or verify an individual's eligibility to receive a health service,

iii. to conduct investigations, discipline proceedings, practice reviews or inspections,

iv. to conduct research (with the approval of an appropriate ethics committee),

v. to provide education for health service providers,

vi. to carry out a purpose authorized or required by legislation (e.g. Public Health Act; Child, Youth and Family Enhancement Act) or

vii. for internal management purposes, including planning, resource allocation, policy development, quality improvement/quality assurance, monitoring, audits, evaluation, reporting and to manage human resources.

Disclosure of Health Information

4.4 The express wishes of the individual together with any other relevant factors are to be considered before any disclosure [HIA, section 58(2)]. As a result, individuals may specify if they do not wish certain pieces of health information to be disclosed. Masking of health information in Alberta Netcare is also possible (see Section 8).

4.5 Any time health information is disclosed the authority and identity of the recipient is authenticated (e.g. disclosing health information over the phone).

4.6 Health information may only be disclosed without consent in limited circumstances (HIA s. 35), including:

i. to another custodian, or its affiliate, for any of the Authorized Uses and in some situations to the government of Canada or of another province or territory for the government's use for health system planning/management and health policy development;

ii. to a person who is responsible for providing continuing care and treatment to the individual;

iii. to family members of the individual, or a close personal friend, if the information is provided in general terms and concerns the presence, location, condition, diagnosis, progress and prognosis of the individual on the day on which the information is disclosed, unless contrary to the express request of the individual;

iv. to contact family members or a close personal friend of the individual, if the individual is injured, ill or deceased, unless contrary to the express request of the individual;

v. if the individual is deceased, to the family members of the individual or a close personal friend, if the information relates to the circumstances surrounding the death of the individual or to health services recently received by the individual, unless contrary to the express request of the individual;

vi. for the purpose of a court proceeding to which the custodian is party;

vii. to comply with a subpoena, warrant or court order issued or made by a court, person or body having jurisdiction in Alberta;

viii. to any person if the custodian believes, on reasonable grounds, that the disclosure would avert or minimize an imminent danger to the health or safety of any person; or

ix. if the individual lacks mental capacity to consent and, in the opinion of the custodian, disclosure is in the best interest of the individual.

x. to third party insurers in order to obtain or process payment and to adjudicate health product and service claims more effectively.

xi. to the College of Physicians and Surgeons of Alberta for the purpose of administering the Triplicate Prescription Program.

4.7 Health information may be disclosed without consent to a health professional body under section 35(4) of HIA for the purpose of an investigation, discipline proceeding, practice review or inspection. In such cases, the health professional body must agree in writing not to disclose the information except as authorized by its governing legislation.

4.8 Health information may be disclosed without consent to prevent or limit fraud or abuse of health services under section 37(1) of HIA:

i. The custodian may disclose individually identifying health information referred to in policy 4.9 without the consent of the individual who is the subject of the information to a police service or the Minister of Justice and Attorney General where the custodian reasonably believes;

- that the information relates to the possible commission of an offence under a statue or regulation of Alberta or Canada, and
- that the disclosure will detect or prevent fraud or limit abuse in the use of health services.

4.9 The custodian may disclose the following information under policy 4.7:

i. the name of an individual,
ii. the date of birth of an individual,
iii. the personal health number of an individual,
iv. the nature of any injury or illness of an individual,
v. the date on which a health service was sought or received by an individual,
vi. the location where an individual sought or received a health service,
vii. the name of any drug, as defined in the *Pharmaceutical Profession Act*, provided to or prescribed for an individual and the date the drug was provided or prescribed.

4.10 If the custodian discloses health information about an individual under policy 4.7, the custodian may also disclose health services provider information from whom that individual sought or received health services if that information is related to the information that was disclosed.

4.11 Health services provider information may be disclosed under policy 4.10 without the consent of the health services provider who is the subject of the information.

4.12 Health information may be disclosed without consent to prevent or limit fraud or abuse of health services providers under section 37(2):

i. the custodian may disclose health information about an individual referred to in policy 4.13 without the consent of the health services provider who is the subject of the information to a police services or the Minister of Justice and Attorney General where the custodian reasonably believes;

- that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada by the health services provider, and
- that the disclosure will detect or prevent fraud or limit abuse in the provision of health services.

4.13 The custodian may disclose the following information under policy 4.12:

i. the name of the health services provider;

ii. the business address of the health services provider;

iii. the date on which the health services provider provided a health service;

iv. the description of a health service provided by the health services provider;

v. the benefits that were paid or charged in relation to a health service provided by the health services provider.

4.14 If the custodian discloses information under policy 4.12 about a health service, the custodian may also disclose health information about the individual who received that health service if that information is related to that health service.

4.15 Health information that identifies an individual may be disclosed under policy 4.14 without the consent of the individual who is the subject of the information.

4.16 Health information may be disclosed without consent to protect public health and safety under section 37(3) of HIA:

i. the custodian may disclose individually identifying health information referred to in policy 4.17 without the consent of the individual who is the subject of the information to a police service or the Minister of Justice and Attorney General where the custodian reasonably believes;

- that the information relates to the possible commission of an offence under a statue or regulation of Alberta or Canada, and
- that the disclosure will protect that health and safety of Albertans.

4.17 The custodian may disclose the following information under policy 4.16:

i. the name of an individual;

ii. the date of birth of an individual;

iii. the date on which a health service was sought or received by an individual;

iv. the location where an individual sought or received a health service;

v. whether any samples of bodily substances were taken from an individual.

4.18 If the custodian discloses health information about an individual under policy 4.16, the custodian may also disclose health services provider information about a health services provider from whom that individual sought or received health services if that information is related to the information that was disclosed under policy 4.16.

4.19 Health services provider information may be disclosed under policy 4.18 without the consent of the health services provider who is the subject of the information.

4.20 As required under section 41 of HIA, when a record containing individually identifying diagnostic, treatment and care information is disclosed without consent, the section 41 notation form is to be completed (see Appendix 8) and retained for 10 years after the disclosure. A computer notation of the information disclosure shall be recorded on the individual's record.

4.21 Unless health information is disclosed under one of the situations listed above or is disclosed directly to the individual or his/her Authorized Representative, consent is required.

4.22 As required under section 42 of HIA, when any individually identifying diagnostic, treatment and care information is disclosed whether the disclosure is made with or without consent, the recipient is notified in writing of the purpose of the disclosure and the authority under which the disclosure is made (i.e. which section of HIA allows the disclosure). This obligation to notify does not apply to disclosures to other custodians, or their affiliates, for any of the Authorized Uses including disclosures to prevent or limit fraud or abuse of health services (see Appendix 9). This notification obligation also does not apply to disclosures made under section 37.1, 37.2, and 37.3.

4.23 Requirements of a valid consent

i. under HIA, consent for the disclosure of health information must be in writing either on paper or electronically and must include the information found in Appendix 10.

Policy 5

Information Privacy and Security in Contracting

5.1 Requirements as Custodian

i. An HIA specific agreement or contract is completed and signed by all service providers who have access to the health information (this does not need to be a separate agreement – HIA specific clauses could be included in a broader contract or service agreement).

ii. Until a contract detailing information privacy and security provisions is executed, the service provider is not allowed to access health information.

iii. When developing contracts with service providers who require access to health information provisions addressing the following are incorporated as required:

- identifying the types of records provided, collected, created, or maintained in order to deliver the service;
- specifying any applicable privacy legislation (e.g. HIA, FOIP, PIPA, PIPEDA);
- identifying the custodian as having custody and control of the health information, including the responsibility and process for handling requests for access to information;
- ensuring that the service provider meets or exceeds the standards set out in HIA and your policies and procedures; and
- specifying the audit or enforcement measures you will undertake to ensure that service providers comply with information privacy and security provisions outlined in contractual agreements, e.g. non-disclosure agreements, audit trails, regular review of service provider access requirements.

5.2 Service Provider's Requirements as Contractor

The Service provider must:

i. Ensure that the service provider's information security and privacy policies are available upon request, including any updates or revisions that occur after execution of the contract;

ii. Document service provider roles and responsibilities for carrying out specific information security processes;

iii. Ensure that employees of the service provider are aware of, and understand their responsibility to adhere to, all policies and procedures;

iv. Agree that the service provider and employees who have access to health information must sign a specific non-disclosure agreement;

v. Agree to immediately report to the custodian breaches of confidentiality and privacy;

vi. Identify disaster recovery procedures and backup or any information assets and systems in the custody of the service provider;

vii. Address the retention and disposition (e.g. destruction or return) of all information assets (e.g. records, hardware, system documentation) upon termination of the contract; and

viii. Agree to assist the custodian in fulfilling individuals' access requests for health information within legislated time limits, if necessary.

Policy 6

Research

6.1 All requests for access to personal health information for research purposes must be in writing and accompanied by documentation indicating that the research proposal was reviewed and approved by an appropriate research ethics board.

6.2 The following committees and boards are designated as a research ethics board for this purpose:

i. Alberta Cancer Research Ethics Committee (Alberta Health Services)

ii. College of Physicians and Surgeons of Alberta – Research Ethics Review Committee

iii. Alberta Innovates – Health Solutions – Community Research Ethics Board of Alberta

iv. University of Alberta – Health Research Ethics Board

v. University of Calgary – Conjoint Health Research Ethics Board

vi. University of Lethbridge – Human Subject Research Committee

6.3 Upon receipt of the request and a copy of the ethics approval, a decision to disclose the health information to the researcher may be made.

6.4 If the decision to disclose the health information is made, the researcher must agree to abide by any conditions suggested by the ethics committee or the Privacy Officer (including obtaining any consents for disclosure that may be required).

6.5 If a decision to disclose health information for research purposes is made, the researcher must enter into an agreement in which the researcher agrees to:

i. Comply with the provisions of HIA and any applicable regulations;

ii. Comply with any conditions imposed regarding the use, protection, disclosure, return or disposal of the health information, if any;

iii. Comply with any requirements to provide against identification of the subject individuals;

iv. Use the health information only for the proposed research;

v. Ensure that the health information is not published in any form that could lead to the identification of any of the subject individuals involved;

vi. Only contact individuals for additional information if the custodian has first obtained consent to being contacted for that purpose;

vii. Allow access or inspection of the researcher's premises to ensure that the researcher is complying with the terms set out in the agreement; and

viii. Pay any costs levied, which must not exceed the cost of providing the service to the researcher.

Policy 7

Transitory Records

7.1 A record will be defined as a transitory record if it falls into any of the following categories:

i. *Temporary information*: Records required for specific activities but having no further value once the activity has been completed (e.g. phone messages, post-it notes, invitations, and some cover sheets).

ii. *Duplicates*: Exact reproductions of a master document. Note that if the duplicate records have been annotated or altered in any way, it may have become a new record that should be retained (e.g. photocopies, documents scanned into an electronic system).

iii. *Draft Documents and Working Materials*: Including source materials used in preparation of documents and earlier versions of final documents (e.g. drafts of reports, working notes or tapes).

7.2 Transitory records are identified and destroyed after the actions to which they relate or immediate purposes are completed.

7.3 Where practical, transitory records are maintained separate from non-transitory records if they need to be retained for any length of time.

7.4 All confidential transitory records are kept secure and disposed of using containers or shredders designated for confidential records disposal.

7.5 The destruction of transitory records does not need to be documented by listing the records or having a staff member sign off the destruction. Any staff member may destroy transitory records.

7.6 Before destroying documents be sure that the documents are in no way needed for future accountability, liability or documentation purposes.

Policy 8

Alberta Electronic Health Record (Alberta Netcare)

8.1 Alberta Netcare is the provincial integrated health information system established to provide shared access to health information by authorized custodians and their affiliates, in a secure environment. Custodians wishing to participate in Alberta Netcare must sign an Information Management Agreement with Alberta Health.

8.2 The CARNA regulated member who is a custodian and affiliates in the practice setting may only access and use the information available in Alberta Netcare for authorized purposes such as:

i. providing a health service

ii. determining/verifying a person's eligibility to receive a health service

iii. carrying out any purpose set out in the Information Exchange Protocol (IEP) that is an authorized use under the HIA

8.3 The CARNA regulated member who is a custodian and affiliates in the practice setting accessing Alberta Netcare must use their own unique user credentials for each access.

8.4 Each user of the Alberta Netcare must log out and close the browser before leaving the system;

i. the custodian will ensure all users are trained to log off their session.

ii. if a user comes across an open session of Alberta Netcare, he/she must alert the custodian. The custodian must take appropriate action to ensure that a similar scenario does not happen again in the future. The user of the forgotten open session must be logged out and the browser closed. A new session must then be initiated by the new user using his/her fob.

8.5 Masking – If an individual makes an express wish to limit their health information from being accessed, it is possible to honor such a request via masking of their health information in the Alberta EHR. Detailed information regarding the process for Global Person-Level Masking and related forms are available on the Alberta Netcare login page.

Policy 9

Penalties/Sanctions

9.1 If a policy is wilfully or accidentally breached, penalties/sanctions may include disciplinary action, up to and including dismissal.

Policy 10

Distribution

10.1 A copy of these policies and procedures will be distributed to all staff as well as all students, volunteers and contracted personnel in the practice setting. Currently there are _____ copies in circulation with the last date of revision being _____.

10.2 Following updates, previous copies will be removed and only the most current revision shall be available for circulation or reference by staff.

Policy 11

Approval

11.1 As the _____ (title of staff member authorized to approve or distribute policies) I have read and understood these as being current and complete.

_____ _____

Print name Date

_____

Signature

Appendix 1

HIA Definitions

Affiliates: Includes all employees, volunteers, information managers, students and persons contracted to provide services for custodians.

Collection: When a custodian, or its affiliate, gathers, acquires, receives or obtains health information.

Consent: Agreement by an individual to the disclosure of his/her health information. To be valid, consent must be provided in writing or electronically and must include:

- an authorization for the custodian to disclose the health information specified in the consent;
- the purpose for which the health information may be disclosed;
- the identity of the person to whom the health information may be disclosed;
- an acknowledgment that the individual providing the consent has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent;
- the date the consent is effective and the date, if any, on which the consent expires, and
- a statement that the consent may be revoked at any time by the individual providing it.

Control: The authority to exercise control over or to manage the record or information, including restricting, regulating and administering its use, disclosure and disposition.

Custodians: Include the following:

- Regional Health Authorities (Alberta Health Services)
- Other nursing homes not owned by the above.
- Provincial health boards (e.g. Health Quality Council of Alberta)
- Minister and the Department of Health and Wellness.
- Licensed pharmacies
- Regulated health professionals identified in HIA and HIA regulations, including pharmacists, physicians, chiropractors, midwives, dentists, dental hygienists, denturists, nurses, opticians, optometrists and podiatrists
- Others as listed in HIA and the HIA regulations.

Custody: Physical possession of the health record or information.

Disclosure: When a custodian, or its affiliate, shares health information with i) another custodian, or ii) a third party (i.e. a person that is neither a custodian or an affiliate).

Health Information: Recorded information about an individual falling under any or all the following categories: i) Registration Information, ii) Diagnostic Treatment and Care Information,

Health service: 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 regulation.

Individually Identifying: When used to describe health information, means that the identity of the individual who is the subject of the information can be readily determined from the information.

Information Manager: Means a person or body that (a) processes, stores, retrieves or disposes of health information (b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, and (c) provides information management or information technology services. (HIA s 66(1))

Record: Health information in any form, including notes, images, audiovisual recordings, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner. Excludes: software and any mechanism that produces records.

Research: Means academic, applied or scientific health-related research that necessitates the use of individually identifying diagnostic, treatment and care information or individually identifying registration information, or both.

Use: To apply health information for a purpose and includes reproducing information, but does not include disclosing information. Making *prescribed* health information available through the Alberta EHR, and accessing information through the Alberta EHR are considered *use* of health information.

Appendix 2

Privacy and Management of Health Information: Standards for CARNA's Regulated Members

Safeguarding and promoting your clients' rights is a professional responsibility. Ensuring clients' values and wishes are understood and respected may involve ethical responsibilities and/or legislative obligations. This document was written to provide direction for regulated members on the expectations for the appropriate collection, use and disclosure of health information in their custody and control. Please see the CARNA website for access to this document and other Health Information Act Resources.

You may also find it useful to access the online learning privacy modules. The learning modules can be found here.

Appendix 3

Request to Access Health Information and/or Access Log

(Adapted from Health Information Act: Guidelines and Practices, Alberta Health and Wellness, 2001)

The information on this form is collected under Alberta's *Health Information Act* and will be used to respond to your request for health information and/or a record of who has accessed your health information in the pharmacy system.

Last Name First Name

Mailing Address

City or Town Province Postal Code

Telephone (Business) Telephone (Home)

Fax number E-mail Address

Date of Birth (d/m/y) Other

Provide a description of the information you want to access, in as much detail as possible. Indicate if you also want access to records about the disclosure of your information. Be sure to give all your previous names. (If you are requesting access to another individual's information you must either: i) be that individual's *Authorized Representative*, see below, or ii) attach a valid section 34 consent executed by that individual).

Please indicate if you wish to:

- ☐ **Receive a photocopy of the specified record**
  Please note that a base fee of $25 applies. For convenience, you may enclose this fee with your request. You should be provided with an estimate of any additional costs.

- ☐ **View the original record, without receiving a copy**
  Please ask for an estimate of the fee you will pay for:
  - review of the original by the CARNA regulated member and/or
  - supervision by CARNA regulated member or designated staff person of your review

A deposit of 50% of the fee may be required.

Signature Date

If you are executing this Request to Access Health Information as an *Authorized Representative*, you must check the box that applies to you and provide a copy of documentation that supports your authority:

- ☐ if the individual is 18 years of age or older, by the individual
- ☐ if the individual is under 18 years of age and understands the nature of the right or power and the consequences of exercising the right or power, by the individual
- ☐ if the individual is under 18 years of age but does not understand the nature of the right or power and the consequences of exercising the right or power, by the guardian of the individual
- ☐ if the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate
- ☐ if a guardian or trustee has been appointed for the individual under the *Adult Guardianship and Trusteeship Act,* by the guardian or trustee if the exercise of the right or power relates to the powers and duties of the guardian or trustee
- ☐ if an agent has been designated under a personal directive under the *Personal Directives Act*, by the agent if the directive so authorizes
- ☐ if a power of attorney has been granted by the individual, by the attorney if the exercise of the right or power relates to the powers and duties conferred by the power of attorney
- ☐ by the individual's nearest relative as defined in the *Mental Health Act* if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act
- ☐ by any person with written authorization from the individual to act on the individual’s behalf

Appendix 4

Refusal by Custodian to make Correction or Amendment

The purpose of the letter is to give written notice to the applicant or their *Authorized Representative* of refusal to make the requested correction or amendment and of the reasons for the refusal.

To:

Last Name	First Name	
Mailing Address		
City or Town	Province	Postal Code
Telephone (Business)	Telephone (Home)	
Fax number	E-mail Address	
Date of Birth (d/m/y)	Other	

Description of the correction or amendment that was requested by the applicant or their *Authorized Representative*.

The requested correction or amendment was not made in respect of:

- ☐ a professional opinion or observation made by a health services provider about the applicant, or
- ☐ a record that was not originally created by that custodian.

Additional rational for refusal to correct or amend information is detailed below;

You may elect to do either of the following, but may not elect both:

(a) ask for a review of this decision by the Privacy Commissioner;

(b) submit a statement of disagreement setting out in 500 words or less the requested correction or amendment and the applicant's reasons for disagreeing with this decision within 30 days of receipt of this letter.

Signature Date

Appendix 5

Request to Correct or Amend Health Information

(Adapted from Health Information Act: Guidelines and Practices, Alberta Health and Wellness, 2001)

The information on this form is collected under Alberta's Health Information Act and will be used to respond to your request for request for correction or amendment.

Last Name First Name

Mailing Address

City or Town Province Postal Code

Telephone (Business) Telephone (Home)

Fax number E-mail Address

Date of Birth (d/m/y) Other

Whose information do you want to correct?

- ☐ your own health information
- ☐ another individual's health information (you must be that individual's *Authorized Representative*, see below)

Provide a description of the information you want to correct or amend, in as much detail as possible. (Be sure to give the complete name that is in the records if it is different from the name given above. If you need more space, please attach a separate sheet of paper).

What correction or amendment do you want to make and why? (Please attach any documents that support your request.)

Signature Date

If you are executing this Request to Correct or Amend Health Information as an *Authorized Representative*, you must check the box that applies to you and provide a copy of documentation that supports your authority:

- ☐ if the individual is 18 years of age or older, by the individual
- ☐ if the individual is under 18 years of age and understands the nature of the right or power and the consequences of exercising the right or power, by the individual
- ☐ if the individual is under 18 years of age but does not understand the nature of the right or power and the consequences of exercising the right or power, by the guardian of the individual
- ☐ if the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate
- ☐ if a guardian or trustee has been appointed for the individual under the *Adult Guardianship and Trusteeship Act,* by the guardian or trustee if the exercise of the right or power relates to the powers and duties of the guardian or trustee
- ☐ if an agent has been designated under a personal directive under the *Personal Directives Act*, by the agent if the directive so authorizes
- ☐ if a power of attorney has been granted by the individual, by the attorney if the exercise of the right or power relates to the powers and duties conferred by the power of attorney
- ☐ by the individual's nearest relative as defined in the *Mental Health Act* if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act
- ☐ by any person with written authorization from the individual to act on the individual’s behalf

Appendix 6

Components for an Affiliate's Oath of Confidentiality

(Adapted from Health Information Act: Guidelines and Practices, Alberta Health and Wellness, 2001)

- A statement, sworn (or affirmed) by the affiliate, stating that:

  1. He/she will uphold to the best of his/her ability his/her duties under the Health Information Act and the regulations and the custodian's policies and procedures; and

  2. He/she will not disclose or make known any recorded or non-recorded health information of an individual except as authorized by HIA, the HIA regulations and the custodian's policies and procedures.

- Space for the city, town, village, etc. where the oath is sworn (or affirmed)

- Space for the date and signature of a witness

- (Optional) Place for a Commissioner for Oaths to commission the swearing (or affirming) of the oath

CONFIDENTIALITY OATH

1) I, _____ agree that I will faithfully discharge my duties as staff, an employee, volunteer or contracted service provider in this practice setting <name of clinic/facility> and will observe and comply with all policies and procedures of the practice setting with respect to privacy, confidentiality, and security of health information.

2) Unless legally authorized to do so, I will not use or disclose health information that comes to my knowledge or possession by reason of my affiliation with the practice setting, including after I cease to be employed in this practice setting.

3) I understand that a breach of this agreement may be just cause for termination of my employment or affiliation in this practice setting.

4) I am aware that the practice setting has policies and procedures regarding the privacy, confidentiality, and security of health information and I understand that it is my responsibility to be familiar with the requirements outlined in these policies and procedures.

5) My use of Netcare and the practice setting's electronic point of service applications may be monitored to ensure appropriate confidentiality and security. Specifically, audit and access logs will be checked by the system administrator if a breach of security or privacy is suspected. The practice setting will work with the vendor to automatically generate audit logs that identify use of the system outside of office hours, same last name (of user and patient record look-up), and similar monitoring criteria.

6) I understand that I can refer to the practice setting Privacy Officer for the details of these policies and any other information required for me to understand my obligations.

_____
Signature

_____
Printed Name

_____
Signed at (Location)

_____
Date

Appendix 7

Sample Mini-poster

COLLECTION OF HEALTH INFORMATION

We are committed to protecting the privacy of your health information and managing your health information in accordance with the Health Information Act (HIA).

HIA requires us to tell you the purposes for which we collect your health information and the legal authority that allows us to collect your health information.

1. The health information we collect from you is required for the purposes of providing you diagnostic, treatment and health care services. We may also collect your health information:

    - to carry out any of the other purposes authorized under section 27 of HIA, including, for example, quality management and the training of health professional students; or

    - if the collection is required by law.

2. We collect your health information pursuant to our legal authority under section 20(b) of HIA.

If you have any questions about how we manage your health information, please contact our Privacy Officer at:

[Privacy Officer's phone number, business address and email address, if applicable]

Appendix 8

Section 41 Notation

Section 41 of HIA requires a notation of the following data when a record of diagnostic, treatment and care information is disclosed without consent: i) the recipient; ii) the date and purpose of the disclosure; and iii) a description of the information.

All such notations must be retained for 10 years from the date of disclosure.

In some cases the notation may already be created and no additional form is required. For example, if a medication history is faxed, mailed or emailed to physician, the fax cover sheet, covering letter or email message would likely already include: the physician's name (the recipient) and a dated cover note such as "Further to your request to confirm medication history for the past month" (the date, purpose, and a description).

If the entire fax is retained for 10 years, the content of the fax would also serve as a description of the information. However, in most cases only the fax cover sheet is retained. If you are unsure if your fax cover sheet, covering letter or email message includes the required data, the following form can be added to your fax, letter or email:

NOTIFICATION PURSUANT TO THE S.41 OF THE
HEALTH INFORMATION ACT

The attached individually identifying diagnostic, treatment and care information of _____ (name of subject individual) is being disclosed to _____ (name of recipient) by _____ (name of custodian) on _____ (date), for the following purpose(s): _____.

Appendix 9

Section 42 Notification

Section 42 of HIA requires that certain recipients be notified in writing of the following data when any form of diagnostic, treatment and care information is disclosed, regardless of consent:

i). the purpose of the disclosure; and
ii). the authority under which the disclosure is made.

This notification does not apply to disclosures between custodians, or their affiliates, for any of the Authorized Uses.

The following form can be given or sent to the recipient: i) separately, if the diagnostic, treatment and care information is disclosed verbally, or ii) attached to a fax, letter or email that discloses the diagnostic, treatment and care information. It lists the most common sections of HIA under which disclosures are made and allows an "Other" category for other situations.

NOTIFICATION PURSUANT TO THE S.42 OF THE
HEALTH INFORMATION ACT

The individually identifying diagnostic, treatment and care information of _____ (name of subject individual) was/is disclosed:

- ☐ verbally
- ☐ in writing as attached
- ☐ in writing not attached

to _____ (name of recipient) on _____(date), pursuant to the following provision of the *Health Information Act*:

- ☐ s.34 (with consent)
- ☐ s.35(1)(m) (to avert or minimize an imminent representative) danger)
- ☐ s.35.(1)(n) (best interests of individual who lacks the mental capacity to consent)
- ☐ s.35(1)(b) (continuing treatment and care)
- ☐ s.35(1)(p) (to comply with an act or regulation of Alberta or Canada
- ☐ s.35(1)(c) (general information to family that authorizes or requires member or person believed to have a close personal relationship – not contrary to express request)
- ☐ s.35(1)(i) (subpoena, warrant or court order)
- ☐ Other _____ (cite application section of the HIA)

NOTE: ABOVE ARE ONLY BRIEF DESCRIPTIONS OF COMMONLY APPLIED HIA PROVISIONS, PLEASE REVIEW HIA PROVISIONS IN FULL FOR APPLICABILITY.

Appendix 10

Consent to the Disclosure of Health Information

SECTION 34 CONSENT PURSUANT TO THE HEALTH INFORMATION ACT

Disclosure of Health Information Authorization

I, _____ (name of Patient) authorize my personal individually identifying:

health information reports (which may infer diagnostic, treatment and care information, registration information, and health services provider information*)

of _____ (name of Patient/Client/Health Services Provider*) to be disclosed by _____ (name of custodian), in accordance with section 34 the Health Information Act to _____ (name of recipient(s), address),

for the following purpose(s):

_____.

I acknowledge that I have been made aware of the reasons for the disclosure of the above information, and the risks and benefits associated with consenting to its release.

I understand that I make revoke my consent at any time, by providing a signed, written statement to that effect.

Dated this ____of _____, _____. Expiry date (if any) ____of _____, _____.
(day) (month) (year) (day) (month) (year)

Signature of Patient

Printed Name of Patient

Signature of Witness

Printed Name of Witness

If you are executing this Consent as an **Authorized Representative**, you must complete the checklist below.

Authorized Representative: Check the box that applies to you and provide a copy of documentation that supports your authority:

- ☐ if the individual is 18 years of age or older, by the individual
- ☐ if the individual is under 18 years of age and understands the nature of the right or power and the consequences of exercising the right or power, by the individual
- ☐ if the individual is under 18 years of age but does not understand the nature of the right or power and the consequences of exercising the right or power, by the guardian of the individual
- ☐ if the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate
- ☐ if a guardian or trustee has been appointed for the individual under the *Adult Guardianship and Trusteeship Act,* by the guardian or trustee if the exercise of the right or power relates to the powers and duties of the guardian or trustee
- ☐ if an agent has been designated under a personal directive under the *Personal Directives Act*, by the agent if the directive so authorizes
- ☐ if a power of attorney has been granted by the individual, by the attorney if the exercise of the right or power relates to the powers and duties conferred by the power of attorney
- ☐ by the individual's nearest relative as defined in the *Mental Health Act* if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act
- ☐ by any person with written authorization from the individual to act on the individual’s behalf

ACKNOWLEDGMENT

CARNA gratefully acknowledges the Alberta Pharmacists' Association (RxA) who willingly shared their privacy and security policies and procedures to use as a template for CARNA privacy and security policies and procedures.