CONTENTS

Contents

Purpose

The collection, use, disclosure, and retention of health information by this clinic are governed by the provisions of the Health Information Act (HIA) as well as requirements of the College of Physicians and Surgeons of Alberta (CPSA). The clinic's privacy policies and procedures have been developed in compliance with the HIA to enable patient care and effective service delivery, while protecting the privacy of patients of the clinic.

Scope

These policies apply to clinic personnel, including physicians, nurses, medical office assistants, residents and medical students.

These policies apply to health information regardless of format and apply to all facilities and/or equipment.

Principles

1. Protecting the confidentiality of health information and the privacy of individuals is ahigh priority. This includes protection against unauthorised use, disclosure, modification, or access to information.

2. Individuals have a right to access information about themselves, subject to limited and specific exceptions.

3. Individuals who believe there is an error or omission in their health information have a right to request to correct or amend the information.

4. When collecting health information from an individual, he/she must be informed of the purpose and authority for the collection, and the title, business address and telephone number of someone who can answer questions about the collection.

5. Health Information is used and disclosed only for the purpose authorized in Section 27 of the HIA unless otherwise authorized or required by law, or with consent of the individual who is the subject of the information.

6. Only the least amount of health information necessary to carry out the intended purpose is collected, used, and disclosed, and is only collected by staff that require the information to perform their assigned duties, i.e. staff must have a 'need to know' in order to access a patient's health information.

7. Health Information is collected, used, and disclosed at the highest level of anonymity possible for the intended purpose.

8. The expressed wishes of the individual, who is the subject of the information, and other relevant factors, are taken into consideration when determining how much health information to disclose.

9. Individuals have the right to request that Alberta Information and Privacy Commissioner review access, privacy and correction decisions made respecting their information.

10. Failure to comply with these information privacy and security policies and procedures may result in penalties or sanctions, including disciplinary action and termination of employment. Individuals may also be subject to prosecution for the contravention of the law.

11. Physicians and their staff adhere to the College of Physicians and Surgeons Code of Ethics, and Standards of Practice including the fundamental responsibilities to protect patient privacy.

Policy Description

1. Roles and Responsibility

1.1. The

1.2. Responsibilities of the Privacy Officer will Include:

1.2.1. Identifying privacy compliance issues in the clinic.

1.2.2. Ensuring that all policies and procedures are developed and maintained.

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

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

1.2.5. Responding to requests for access to health information throughout the clinic.

1.2.6. Ensuring proper retention and disposal of health information as per the CPSA.

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

1.3. All staff, including custodians and affiliates, are responsible for:

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

1.3.2. Collecting, using, and disclosing health information only in the performance of their job duties.

1.3.3. Reading and signing-off on policies and procedures.

1.3.4. Reporting privacy breaches to the Privacy Officer.

1.4. All physicians must adhere to the CPSA Code of Ethics (see Appendix 2) and are responsible for protecting patient privacy.

2. Right of Access

Informal Requests

2.1. Requests from individuals to access basic health information solely about themselves (e.g. confirm a medication recently prescribed or a prescription or view a lab or diagnostic imaging result) are handled informally (with valid identification if uncertain of patient identity). If any part of the disclosure of this information requires explanation, as in the case of test results, an appointment would be made with the clinic physician to review the results.

2.2. Requests from individuals to correct or amend basic health information solely about themselves are handled informally with presentation of valid identification if uncertain of patient identity (e.g. driver's license, Alberta Health Care Insurance Plan Card) and documentation.

Formal Requests

2.3. Requests for access to health information which cannot be handled informally must be made in writing (see Appendix 3). A person may request access to another individual's information only if he or she has:

2.3.1. That individual's written authorization, or

2.3.2. Proof of being that individual's authorized representative (as described in policy 2.12.).

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

2.5. Such requests are recorded in an audit log, which can be viewed by the patient upon request.

PROCEDURE TO REQUEST CORRECTION OF HEALTH INFORMATION

2.6. Requests to correct or amend information which cannot be handled informally must be made in writing (see Appendix 5). 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 or the HIA.

2.6.1. 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 the HIA.

2.6.2. 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).

2.6.3. 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:

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

2.6.4. 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 of 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.

Non-Disclosure (in relation to an access request)

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

2.7.1. If it is about an individual other than the applicant, unless the information was originally provided by the applicant in the context of a health service being provided to the applicant; or the applicant has authority under Section 104 of the HIA to receive the information (e.g. guardian of a minor, executor of an estate for purposes of authorized under the Act) [HIA s11(2)(a)]]

2.7.2. 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

2.7.3. If the disclosure is prohibited by legislation

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

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

2.8.2. Threaten the health or safety of another individual or the public;

2.8.3. Pose a threat to public safety;

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

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

2.9. 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 at the clinic who can answer questions about the severing decisions.

2.10. 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.

2.11. If the applicant views the original record, the clinic privacy officer shall be present to answer questions and maintain the integrity of the record.

Authorized Representatives

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

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

2.12.2. 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,

2.12.3. if the individual is under 18 years if 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

2.12.4. 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,

2.12.5. if a guardian or trustee has been appointed for the individual under the *Dependent Adults 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,

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

2.12.7. 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,

2.12.8. if the individual is a formal patient as defined in the *Mental Health Act*, by the individuals nearest relative as defined in that Act if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act,

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

2.13. 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.

2.14. 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.

2.15. 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.

3. Information Handling and Security

3.1. Administrative Safeguards

3.1.1. 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).

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

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

3.1.4. 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.

3.1.5. Staff members are monitored for compliance with policies and procedures.

3.1.6. All new staff members are required to review policies and procedures, and sign off that they have read, understood and will abide by them.

3.1.7. All staff members are required to attend HIA, and related privacy and security, training sessions (e.g. Regular updates at staff meetings).

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

3.1.9. Termination process for employees and Third Parties – Upon termination of any employee(s) or Third Parties, the following procedures are to be followed:

3.1.9.1. 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;

3.1.9.2. Retrieve all system related documentation;

3.1.9.3. Terminate all user accounts, passwords and alarm codes.

3.1.10. Health information is not transmitted verbally if conversations can be overheard or intercepted.

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

3.1.12. All privacy compliance issues, and security breaches are reported to the Privacy Officer.

3.1.13. Health information is retained in accordance with specific records retention provisions as set out by the College of Physicians and Surgeons of Alberta.

3.2. Technical Safeguards

3.2.1. 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 the job duties (e.g. Windows login).

3.2.2. System administrators must each have an administrator account for performing system administration and a limited privilege account for performing non system administration tasks.

3.2.3. Access to electronic systems is password protected.

3.2.4. 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. @#$%^&). It is preferable not to use words found in the dictionary or names that could easily be guessed, like your pet's name, your name, or your children's name.

3.2.5. Passwords are changed every 3 months as prompted by the system.

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

3.2.7. Confidential business or identifiable health information will not be sent via email over public or external networks without the use of appropriate security measures such as encryption or by the use of a two-factor authentication connection.

3.2.8. To detect unauthorized access and prevent modification or misuse of user data in applications, use of internal network and Netcare will be monitored by the system administrator and Netcare to ensure conformity to access policies and standards. Audit and access logs will be checked by the system administrator if a breach of security or privacy is suspected.

3.2.9. If a wireless network is implemented, it will be set up according to the requirements established by the Physician custodian.

3.2.9.1. The access device will be securely fastened on an inside wall of the clinic in a non-public access area (e.g. dispensary).

3.2.9.2. Either WPA or WPA2 encryption will be used.

3.2.9.3. The default SSID will be changed, and the SSID broadcast disabled.

3.2.9.4. Default administrator passwords and usernames will be changed to a unique username and strong pass phrase. Access to the username and password will be restricted to the physician custodian and authorized contracted IT support.

3.2.9.5. Firewalls will be enabled for the access device and all computers.

3.2.9.6. Connection to the wireless system will be authorized by the physician custodian and clinic Privacy Officer.

3.2.10. Use of any mobile computing devices (e.g. laptops, iPads, USBs, portable hard drives) must be authorized by the physician custodian.

3.2.10.1. The physician custodian will determine what staff members are allowed to access via their mobile device (e.g. drug information website).

3.2.10.2. If a mobile device is used to store any patient information, it must be protected by full disk encryption.

3.2.10.3. All mobile devices that have the capability should be secured with Alberta Health compliant passwords, PINs or other login requirements.

3.2.10.4. When not in use, mobile devices should be securely stored in the no-public access area of the clinic (e.g. locked drawer or cabinet).

3.2.10.5. If transporting a mobile device to/from the clinic, the device should be locked in the trunk of the care at the point of departure.

3.2.10.6. An inventory of mobile devices owned by the clinic will be maintained by the physician custodian, (e.g. MAC addresses, serial numbers).

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

3.2.11.1. user identification associated with an access

3.2.11.2. role or job function of user

3.2.11.3. date and time of an access

3.2.11.4. actions performed by the user (e.g. creating, viewing, editing, deleting)

3.2.11.5. identification of the individual whose record was accessed (e.g. name, personal health number)

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

3.2.13. Audit trails are reviewed as deemed necessary by the custodian (at minimum on an annual basis), and on an incident basis.

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

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

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

3.2.17. For non-operating systems, the custodian will ensure that software is reviewed on a regular basis and patched as needed.

3.2.18. Electronic systems are backed up on a daily basis.

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

3.2.20. 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.

3.2.21. 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.

3.3. Physical Safeguards

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

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

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

3.3.4. The distribution of keys is strictly controlled; keys are returned by staff after their employment has been terminated.

3.3.5. Building premises are protected by building alarms. Alarm codes are changed as deemed necessary by the custodian and past employee codes are deleted.

3.3.6. Health information, including prescriptions, and test results is not left unattended in areas to which the public has access.

3.3.7. Computer monitors are positioned so that on-screen information cannot be viewed by passers-by.

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

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

3.3.10. 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.

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

3.3.12. Fax machines are located in a secure area.

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

3.3.14. 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 clinic if sent to the wrong number.

3.3.15. 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.

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

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

3.3.18. All information is wiped clean with an appropriate disk wiping utility prior to disposal of electronic data storage devices (e.g. surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMS) or the device(s) and storage medium be physically destroyed.

3.4. Security breaches

3.4.1. All security breaches or privacy compliance issues are reported to the Privacy Officer.

3.4.2. 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.

3.4.3. 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.

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

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

4. Collection, Use and Disclosure of Health Information

4.1. Collection of Health Information

4.1.1. Individually identifying health information is collected directly from the individual who is the subject of the information, or his/her Authorized Representative, unless:

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

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

4.1.1.3. direct collection is not reasonably practicable;

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

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

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

4.1.1.7. the information is publicly available; or

4.1.1.8. the information is disclosed in accordance with Part % of the HIA (the disclosure rules).

4.1.2. A poster is displayed in the clinic 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).

4.2. Use of Health Information

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

4.2.1.1. to provide health services;

4.2.1.2. to determine or verify and individual's eligibility to receive a health service;

4.2.1.3. to conduct investigations, discipline proceedings, practice reviews or inspections;

4.2.1.4. to conduct research (with the approval of an appropriate ethics committee);

4.2.1.5. to provide education for health service providers;

4.2.1.6. to carry out a purpose authorized or required by legislation (e.g. Public Health Act, Child Welfare Act); or

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

4.3. Disclosure of Health Information

4.3.1. As required under section 58(2) of the HIA, the express wishes of the individual together with any other relevant factors are considered before any disclosure. 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).

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

4.3.3. As authorized under section 35 of the HIA, health information may only be disclosed without consent in limited circumstances, including:

4.3.3.1. 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;

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

4.3.3.3. 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;

4.3.3.4. 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;

4.3.3.5. 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;

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

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

4.3.3.8. 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

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

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

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

4.3.3.12. To the successor custodian of Dr. Harvey Sternberg or the attending physician.

4.3.4. Health information may be disclosed without consent to a health professional body under section 35(4) of the 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.

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

15

4.3.5.1. The custodian may disclose individually identifying health information referred to in policy 4.3.5.2 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;

4.3.5.1.1. that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada, and

4.3.5.1.2. that the disclosure will detect or prevent fraud or limit abuse in the use of health services.

4.3.5.2. The custodian may disclose the following information under policy 4.3.5.1:

4.3.5.2.1. the name of the individual;

4.3.5.2.2. the date of birth of an individual;

4.3.5.2.3. the personal health number of an individual;

4.3.5.2.4. the nature of any injury or illness of an individual;

4.3.5.2.5. the sate on which a health service was sought or received by an individual;

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

4.3.5.2.7. 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 on prescribed.

4.3.5.3. If the custodian discloses individually identifying health information about an individual under policy 4.3.5.1, 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 4.3.5.1.

4.3.5.4. Health services provider information may be disclosed under policy 4.3.5.3 without the consent of the health services provider who is the subject of the information.

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

4.3.6.1. The custodian may disclose individually identifying health information referred to in policy 4.3.6.2 without the consent of the health services provider who is the subject of the information to a police service or the Minister of Justice and Attorney General where the custodian reasonably believes;

4.3.6.1.1. 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

4.3.6.1.2. that the disclosure will detect or prevent fraud or limit abuse in the provision of health services.

4.3.6.2. the custodian may disclose the following information under policy 4.3.6.1:

4.3.6.2.1. the name of the health services provider;

4.3.6.2.2. the business address of the health services provider;

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

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

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

4.3.6.3. If the custodian discloses information under policy 4.3.6.1 about a health service, the custodian may also disclose individually identifying health information is related to that health service.

4.3.6.4. Individually identifying health information may be disclosed under policy 4.3.6.3 without the consent of the individual who is the subject of the information.

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

4.3.7.1. The custodian may disclose individually identifying health information referred to in policy 4.3.7.2 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;

4.3.7.1.1. that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada, and

4.3.7.1.2. that the disclosure will protect that health and safety of Albertans.

4.3.7.2. The custodian may disclose the following information under policy 4.3.7.1:

4.3.7.2.1. the name of an individual;

4.3.7.2.2. the date of birth of an individual;

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

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

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

4.3.7.3. If the custodian discloses individually identifying health information about an individual under policy 4.3.7.1, the custodian may also disclose health services provider information about a health services provider from whom that individual sought or received health serviced if that information is related to the information that was disclosed under policy 4.3.7.1.

4.3.7.4. Health services provider information may be disclosed under policy 4.3.7.3 without the consent of the health services provider who is the subject of the information.

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

4.3.9. 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.

4.3.10. As required under section 42 of the HIA, wen 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 the HIA allows the disclosure). This notification obligation 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 7). This notification obligation also does not apply to disclosures made under sections 37.1, 37.2, and 37.3.

4.4. Requirements of a valid consent

4.4.1. Under the HIA, consent for the disclosure of health information must be in writing on paper or electronically and must include the information found in Appendix 8.

5. Information Privacy and Security in Contracting

5.1. Requirements as Custodian

5.1.1. 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). This agreement will bind the contractor to the clinic's information security policies and procedures or will include specific information security provisions for the contractor.

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

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

5.1.3.1. Identifying the types of records provided, collected, created, or maintained in order to deliver the service;

5.1.3.2. Specifying any applicable privacy legislation (e.g. HIA, FOIP, PIPA, PIPEDA);

5.1.3.3. Identifying the custodian as having custody and control of the health information, including the responsibility and process for handling requests for access to information;

5.1.3.4. Ensuring that the service provider meets or exceeds the standards set out in the HIA and your policies and procedures; and

5.1.3.5. Specify 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, audits trails, regular review of service provider access requirements.

5.2. Service Provider's Requirements as Contractor

5.2.1. The service provider must:

5.2.1.1. 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;

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

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

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

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

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

5.2.1.7. 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

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

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 research ethics boards for this purpose:

6.2.1. Alberta Innovates – Health Solutions – Health Research Ethics Board of Alberta

6.2.2. University of Alberta – Health Research Ethics Board

6.2.3. University of Calgary – Conjoint Health Research Ethics Board

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:

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

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

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

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

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

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

6.5.7. 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

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

7. **Transitory Records**

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

7.1.1. *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).

7.1.2. *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).

7.1.3. *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.

8. Penalties/Sanctions

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

9. Distribution

10.1. A copy of these policies and procedures will be distributed to all clinic staff members as well as the building manager and the janitorial department. Currently there are 2 copies in circulation with the last date of revision being May 15, 2024.

10. **Approval**

11.1. As the Clinic Privacy Officer, I have read and understood these as being current and complete.

Date: April 1, 2024

Christine Waugh

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 the HIA and HIA regulations, including pharmacists, physicians, chiropractors, midwives, dentists, dental hygienists, denturists, nurses, opticians, optometrists and podiatrists
- Others as listed in the 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:

- Protecting, promoting or maintaining physical and mental health
- Preventing illness
- Diagnosing and treating illness
- Rehabilitation
- 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 ascertained from the information.

Information Manager: Means a person or body that i) processes, stores, retrieves or disposes of health information ii) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, and iii) 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.

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.