Privacy Audit Policy

Intent

Protecting the privacy and confidentiality of personal information is an important aspect of the way HIV/AIDS Resources and Community Health ARCH conducts its business. The collection and maintenance of personal information in an appropriate, responsible, and ethical manner is fundamental to ARCH's daily operations.

ARCH will conduct privacy audits at regular intervals, taking an inventory of all personal information holdings, identifying information needs of various functions of the organization and identifying current information practices (including why and how information is collected, used and disclosed).

Applicability

This Privacy Audit Policy informs everyone of ARCH's commitment to privacy and establishes the methods by which privacy audits are conducted. This Privacy Audit Policy applies to all personal information within ARCH's possession and control.

Personal information such as but not limited to is defined as any identifying information about an individual or group of individuals, including name, date of birth, address, phone number, e-mail address, social insurance/security number, nationality, gender, health history, financial data, credit card numbers, bank account numbers, assets, debts, liabilities, payment records, credit records, loan records, opinions, and personal views.

Business information such as but not limited to is defined as ARCH’s business address, business telephone number, name(s) of owner(s), executive officer(s), and director(s), job titles, business registration numbers, and financial status. Business information is treated and handled with the same level of confidentiality, privacy, and respect as personal information.

Procedures

Privacy audits are an internal function of ARCH. The purpose of the audit is to provide ARCH with a full and accurate inventory of information holdings for analysis with respect to any relevant privacy legislation. Any ARCH employees involved in the auditing process will be instructed that there are no right or wrong answers to questioning, and that any information they provide will be held in confidence on a need to know basis. ARCH is under no obligation to make public any findings.
The privacy audit will examine ARCH's information management policies, as well as any existing records in hardcopy, computerized databases, online storage facilities and any other media with regards to employees, partners, customers, shareholders, contractors etc. It will determine how each function of ARCH acquires, makes use of, and discloses any personal information, and who is responsible for the management of that information.

ARCH will document and analyze why personal information has been collected, as well as who has access to that information and for what purposes they have been granted that access in order to ensure that ARCH information management practices comply with relevant privacy legislation.

The privacy audit will be conducted annually by ARCH's Executive Director (Tom Hammond)
Any questions or concerns regarding this Privacy Audit Policy can be addressed by contacting us at 519 763-2255 ext. 129, director@archguelph.ca. ARCH will investigate and respond to concerns about any aspect of the handling of personal information. This organization will address all questions and concerns.

3.3.13 Bill 119, Health Information Protection Act (PHIPA) Policy

Intent

This policy is intended to ensure that ARCH complies with changes to Ontario's *Personal Health Information Protection Act*, *2004* (PHIPA) resulting from Bill 119, *Health Information Protection Act*, *2016,* by establishing guidelines for the collection, use, and disclosure of personal health information of patients/participants of ARCH.

Definitions

Consent directive – An individual makes a consent directive when they withhold or withdraw, in whole or in part, their consent to the collection, use, and disclosure of their personal health information by means of the electronic health record by a health information custodian for the purposes of providing or assisting in the provision of health care to the individual.

Electronic/paper health records – The electronic/paper systems that are developed and maintained for the purpose of enabling the organization, as a health information custodian, to collect, use, and disclose personal health information.

Health information custodian – A person or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work, if any. This includes a health care practitioner or a person who operates a group practice of health care practitioners, and a person who operates a centre, program, or service for community health or mental health whose primary purpose is the provision of health care.

Use – In relation to personal health information in the custody or under the control of a health information custodian or a person, means to view, handle, or otherwise deal with the information, but does not include to disclose the information, and "use," as a noun, has a corresponding meaning.

Information and Privacy Commissioner of Ontario - Is an officer of the Legislature. The commissioner is appointed by and reports to the Legislative Assembly of Ontario and is independent of the government of the day.

Personal Health Information Protection Act, 2004

ARCH's Operating Guidelines

ARCH will comply with practices and procedures:

- That protect the privacy of the individuals whose personal health information it receives and will maintain the confidentiality of the information; and
- That are consistent with the legislation provided by the Information and Privacy Commissioner of Ontario.

Electronic Health Records

ARCH will develop and maintain electronic health records in accordance with PHIPA and the regulations made under the Act. The following guidelines have been implemented in order to ensure compliance with applicable legislation.

When working with electronic and other forms of paper health records such as appointments, lab slips, requisitions etc., ARCH will:

- Manage and integrate personal health information it receives from health information custodians. For example completing full description of patient interactions in EMR.
- Ensure the proper functioning of the electronic health record by servicing the electronic systems that support the electronic health record.
- Ensure the accuracy and quality of the personal health information by conducting data quality assurance activities on the personal health information it receives from health information custodians.
- Conduct analyses of the personal health information in order to provide alerts and reminders to health information custodians for their use in the provision of health care.
- Take reasonable steps to limit the personal health information ARCH receives to that which is reasonably necessary for developing and maintaining the patient/participant electronic health record.
- Prevent employees or any other person acting on behalf of ARCH to view, handle, or otherwise deal with the personal health information received from health information custodians, unless the employee or person acting on behalf of ARCH is involved in the patient/participants care and has been trained in PHIPA.
- Make available to the public and to each health information custodian that provides personal health information to ARCH, intake forms that will include a plain language description of the electronic health record, including all safeguards in place to:
    - → Protect against theft, loss, and unauthorized collection, use, or disclosure of the personal health information;
    - → Protect the personal health information against unauthorized copying, modification, or disposal; and
    - → Protect the integrity, security, and confidentiality of the personal health information; and
    - → Any organizational directives, guidelines, and policies that apply to the personal health information, to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial, or labour relations information.
- Ensure that any third party ARCH retains to assist with providing services for developing or maintaining the electronic health record agrees to comply with the restrictions and conditions that are necessary to enable ARCH to comply with all of the requirements provided in PHIPA.

Recordkeeping

In order to meet its recordkeeping requirements under PHIPA, ARCH will:

- Keep an electronic record of all instances where all or part of the personal health information that is accessible by means of the electronic health or paper record is viewed, handled, or otherwise dealt with, and ensure that the record identifies the information required by section 55.3.4 of PHIPA.

- Keep an electronic record of all instances where a consent directive is made, withdrawn, or modified, and ensure that the record contains the information specified in section 55.3.5 of PHIPA.
- Keep an electronic record of all instances where all or part of the personal health information that is accessible by means of the electronic health record is disclosed with the express consent of the individual and ensure that the record identifies the information required by section 55.3.6 of PHIPA.
- Staff will audit annually and monitor the electronic records that it is required to keep.
- Provide electronic records to the Commissioner upon request as required by PHIPA.
- Provide the records required by a health information custodian to audit and monitor its compliance with PHIPA, upon the health information custodian's request.

Assessment of Threats, Vulnerabilities, and Risks and Response to Breaches

In response to threats, vulnerabilities, and risks, and in response to breaches of security features designed to protect the electronic health record, ARCH will:

- Perform an assessment for each system that retrieves, processes, or integrates personal health information that is accessible by means of the paper / electronic health record with respect to:
    - → Threats, vulnerabilities, and risks to the security and integrity of the personal health information; and
    - → How each of those systems may affect the privacy of the individuals to whom the information relates.
- Make available to each health information custodian who provided personal health information to ARCH a written copy of the results of any assessments carried out that relate to the personal health information the custodian provided.
- Notify, at the first reasonable opportunity, each health information custodian who provided personal health information to ARCH if the personal health information that the health information custodian provided is stolen or lost or if it is collected, used, or disclosed without authority.
- Notify the Commissioner, in writing, immediately after becoming aware that personal health information that is accessible by means of the electronic health record:
    - → Has been viewed, handled, or otherwise dealt with by the prescribed organization or a third party retained by the prescribed organization, other than in accordance with the Act or its regulations; or
    - → Has been made available or released by the prescribed organization or a third party retained by the prescribed organization, other than in accordance with the Act or its regulations.
- Notify the individual at the first reasonable opportunity of the unauthorized collection, and include in the notice a statement that the individual is entitled to make a complaint to the Commissioner;

Reporting to the Commissioner

ARCH will submit to the Commissioner, at least annually, a report in the form and manner specified by the Commissioner, and based on or containing any information, other than personal health information, that is kept in the electronic health record that the Commissioner may specify, respecting every instance in which personal health information was disclosed under section 55.7 of PHIPA since the time of the last report.

Consent Directives

Regarding consent directives, ARCH will:

- Comply with the practices and procedures prescribed in the regulations when managing consent directives.
- Have in place and comply with practices and procedures that have been approved by the Minister for responding to or facilitating a response to a request made by an individual in respect of the individual's record of personal health information that is accessible by means of the electronic health record.
- Ensure that health information custodians only collect personal health information under the circumstances defined in subsection 55.7(1), (2), or (3) where personal health information that is accessible by means of the electronic health record is subject to a consent directive made by an individual under subsection 55.6(1).
- Allow an individual at any time to make a directive that withholds or withdraws, in whole or in part, that individual's consent to the collection, use, and disclosure of his or her personal health information by means of the electronic health record by a health information custodian for the purposes of providing or assisting in the provision of health care to the individual.
- Offer assistance to the person in reformulating the directive if the directive does not contain sufficient detail to enable the prescribed organization to implement the directive with reasonable efforts.
- Notify a health information custodian who seeks to collect personal health information that is subject to a consent directive that an individual has made a directive, and shall ensure that no personal health information that is subject to the directive is provided.
- Audit and monitor every instance where personal health information is collected where a consent directive is in place.

Health information custodians working for ARCH may:

- Disclose personal health information that is subject to a consent directive by means of the electronic health record if the custodian who is seeking to collect the information obtains the express consent of the individual to whom the information relates.

Collection, Use, and Disclosure by Custodians

A health information custodian shall not collect personal health information by means of the electronic health records of ARCH except for the purpose of:

- Providing or assisting in the provision of health care to the individual to whom the information relates; or
- Eliminating or reducing a significant risk of serious bodily harm to a person or group of persons, where the health information custodian believes on reasonable grounds that the collection is necessary for this purpose.

A health information custodian may:

- Use or disclose the information for any purpose for which PHIPA permits or requires a custodian to use or disclose personal health information when providing or assisting in the provision of health care to the individual to whom the information relates.
- A health information custodian who collects personal health information in order to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons,

where the health information custodian believes on reasonable grounds that the collection is necessary for this purpose, may only use or disclose the information for the purpose for which the information was collected.

- A health information custodian may collect, use, and disclose prescribed data elements for the purpose of uniquely identifying an individual in order to collect personal health information.
- If a health information custodian requests that ARCH transmit personal health information to the custodian by means of the electronic health record and ARCH transmits the information as requested, the custodian shall comply with all obligations defined in PHIPA with respect to the transmitted information, regardless of whether the custodian has viewed, handled, or otherwise dealt with the information.

Subject to any exceptions or additional requirements as prescribed in legislation, and in addition to any notice that must be given in the case of an unauthorized use or disclosure, if personal health information about an individual is collected without authority by means of the electronic health record, the health information custodian who is responsible for the unauthorized collection must:

- Notify the individual at the first reasonable opportunity of the unauthorized collection, and include in the notice a statement that the individual is entitled to make a complaint to the Commissioner; and
- If the circumstances surrounding the unauthorized collection meet prescribed requirements, notify the Commissioner of the unauthorized collection.

Protection from Liability for Health Information Custodian

A health information custodian working for or with ARCH who, acting in good faith, provides personal health information to ARCH by means of the electronic health record is not liable for damages resulting from:

- Any unauthorized viewing or handling of the provided information, or any unauthorized dealing with the provided information, by ARCH, its employees, or any other person acting on its behalf; or
- Any unauthorized collection of the provided information by another health information custodian.

Collection, Use, and Disclosure of Personal Health Information by Health Information Custodians

Health information custodians are considered to be collecting, using, or disclosing personal health information in the following circumstances:

- When viewing, handling, or otherwise dealing with all or part of an individual's personal health information by means of the electronic health record and that information was provided to the custodian by another health information custodian, the custodian is considered to:
- Be collecting the personal health information when the information is being viewed, handled, or otherwise dealt with for the first time; and
- Be using the personal health information each subsequent time the information is viewed, handled, or otherwise dealt with.

- Whenever a health information custodian views, handles, or otherwise deals with all or part of an individual's personal health information by means of the electronic health record and that information was provided to ARCH by the custodian, the custodian is considered to be using the personal health information.
- When a health information custodian provides health information to ARCH, the custodian is considered to be disclosing the information only when another health information custodian collects the information by means of the electronic health record.

Personal Health Information Excluding the Electronic Health Record

When a health information custodian provides personal health information in error to ARCH or another organization not involving the electronic health record:

- The custodian is not considered to be disclosing the information to the other organization; and
- The other organization is considered not to be collecting the information from the custodian.
- Staff are instructed to shred the information received and notify the custodian who sent the information.