SUBJECT: Privacy	**POLICY #** **PP-07-61**
CATEGORY: Human Resources	**APPROVED:** **June 2005**
POLICY APPLIES TO: All Staff	**REVISED/REVIEWED:** **April 2019**
	PAGES: **17**

PURPOSE:

At Cassellholme privacy is governed by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), and Personal Health Information Protection Act (PHIPA), laws that establishes rules concerning the collection, use and disclosure of personal health information and, accordingly, subject to external scrutiny by the Information and Privacy Commissioner (IPC). As a health information custodian, Cassellholme and its agents (including staff, physicians, students and volunteers) are responsible for ensuring that the personal health information of our residents and clients is treated with respect and sensitivity.

SCOPE/ACCOUNTABILITY:

Accountability for compliance of Cassellholme with the policy rests with the Chief Executive Officer, although other individuals within Cassellholme are responsible for the day-to-day collection and processing of personal health information. In addition, other individuals within Cassellholme are delegated to act on behalf of the Chief Executive Officer, such as the designated Privacy Officer - the Director of HR. Cassellholme is responsible for personal health information in its possession or custody, including information that has been transferred to an agent of Cassellholme. Cassellholme will use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Cassellholme has implemented policies and practices to give effect to this policy, including:

a. Procedures to protect personal health information.

b. Signing of a Confidentiality Agreement by all agents of Cassellholme prior to commencement of employment or affiliation with Cassellholme.

c. Procedures to receive and respond to complaints and inquiries about Cassellholme information practices.

d. Orientating and training staff and communicating to staff and other agents on information about PHIPA policies and practices

e. Responding to requests for access to, or corrections of, personal health information in the custody of Cassellholme.

In compliance with the Personal Health Information Protection Act, Cassellholme will inform residents and clients of the loss, theft or inappropriate access of their personal health information as soon as reasonably possible. Breaches of this policy and related privacy policies may be subject to disciplinary action. Cassellholme and its agents are also subject to the fines and penalties set out in the Personal Health Information Protection Act.

DEFINITIONS:

Agent - A person that, with the authorization of Cassellholme, acts for or on behalf of the organization in respect of personal health information for the purposes of Cassellholme and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by Cassellholme and whether or not the agent is being remunerated. Examples of agents of Cassellholme include, but are not limited to: employees, volunteers, students, physicians, private contractor's, consultants, and vendors.

Circle of Care - A group that includes any person who is involved in the care or treatment of a given patient and who may rely on implied consent for the collection, use, and disclosure of information for the purposes of providing that patient with care;

Consent Directive - Instruction to withhold or withdraw, in whole or in part, consent to the collection, use, or disclosure of personal health information to one or more individuals;

Health Information Custodian - Listed persons or organizations under the Personal Health Information Protection Act, who have custody or control of personal health information as a result of the work they do. As a long-term care home, Cassellholme is considered to be a Health Information Custodian (Personal Health Information Protection Act, 2004, Schedule A).

Personal Health Information (PHI)- Information about an individual whether living or deceased and whether in oral or recorded form. It is information that can identify an individual and that relates to matters such as the individuals physical or mental health, the providing of health care to the individual, payments or eligibility for health care in respect

of the individual, the donation by the individual of a body part or bodily substance and the individuals health number. (Personal Health Information Protection Act, 2004, section 4.1) Personal health information can be information about a care provider, a staff person, a resident or client of the Home, or a family member of a resident or client. Examples of personal health information include a name, health insurance number, address, telephone number, and personal health information related to care such as care plans and consultation notes, etc.

Substitute Decision-Maker (SDM) - a person who is authorized under PHIPA to consent on behalf of a resident/client to the collection, use, or disclosure of that patient's PHI; and.

Record of Personal Health Information - The Personal Health Information Protection Act defines a record as personal health information in any form or in any medium whether in written, printed, photographic or electronic form or otherwise. Personal health information includes, but is not limited to:

1. the physical or mental health of the individual, including information that consists of the health history of the individual's family;
2. the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;
3. a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual;
4. payments or eligibility for health care in respect of the individual;
5. relates to the donation by the individual of any body part or bodily substance;
6. is the individual's health number, or;
7. identifies an individual's substitute decision-maker.

Exception

Personal health information does not include identifying information contained in a record that is in the custody or under the control of a health information custodian if:

a. the identifying information contained in the record relates primarily to one or more employees or other agents of the custodian; and

b. the record is maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employees or other agents. 2004, c. 3, Sched. A, s. 4 (4).

Identifying Purposes for the Collection of Personal Health Information

Cassellholme shall identify the purposes for which personal health information is collected. Permitted purposes are the delivery of direct resident / client care, employment, benefits and other rentitlements pursuant to the employment relationship, to facilitate business transactions as required, and legal and regulatory requirments.

The identified purposes are specified at or before the time of collection to the individual from whom the personal health information is collected. Depending upon the way in which the information is collected, this can be done verbally or in writing. Cassellholme limits the collection of personal iformation to that which is reasonably necessary for the identified purpose(s). Personal information will be collected only by fair and lawful means

Consent for the Collection, Use & Disclosure of Personal Health Information

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal health information, except where inappropriate.

Note: In certain circumstances, personal health information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. Seeking consent may be impossible or inappropriate, for example when the individual is seriously ill or mentally incapacitated. In these circumstances, consent of the individual's substitute decision maker will be sought, where feasible.

Consent is required for the collection of personal health information and the subsequent use or disclosure of this information. Typically, Cassellholme will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when Cassellholme wants to use information for a purpose not previously identified). Cassellholme will make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Cassellholme will not, as a condition of providing care, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the specified and legitimate purposes. In obtaining consent, the reasonable expectations of the individual are also relevant.

The way in which Cassellholme seeks consent may vary, depending on the circumstances and the type of information collected.

Individuals can give consent in many ways. For example:

a. A form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and specified uses and/or disclosures.

b. Consent may be given verbally when information is collected over the telephone.

c. The consent may be express, implied or given through an authorized representative.

Cassellholme may rely on implicit consent for the disclosure of personal health information to others within a resident/client's circle of care. In cases where express consent is required and it is provided verbally, this exchange is documented in the record of care or personnel file.

We are responsible for complying with the rules on collection, use, and disclosure of information in the various information systems used at Cassellholme Employees, residents, clients or their substitute decision maker are entitled to withdraw consent to the use and disclosure of their personal information by applying a consent directive.

ConnectingOntario ClinicalViewer

In cases of shared technology, in particular, the ConnectingOntario ClinicalViewer may only be accessed for the purpose of providing or assisting in care and may not be accessed for research, quality assurance, or other purposes. Requests by residents/clients for specific consent directives will be documented in a Consent Directive log, and forwarded to the eHealth Pogram Office for processing. Upon approval, the resident/client will be notified that the consent directive is in place. Cassellholme may only override a consent directive with resident/client consent or for authorized purposes per **Appendix B**. We will investigate all overrides of consent directives to ensure the access was appropriate and authorized.

Exception

There are some exceptions to the requirement to obtain consent. These exceptions to the requirement for consent include, but are not limited to, where Cassellholme is required to comply with a court order or investigation by law enforcement personnel.

Limiting Use, Disclosure and Retention

Cassellholme does not use or disclosure personal information for purposes other than those for which it was collected, except with the consent of the individual, or as permitted or required by law. Personal information is retained only as long as is necessary for the fulfillment of those purposes or as required by law.

Cassellholme may disclose personal information to a person or organization involved directly or indirectly in supplying a product or administering a service to clients, resdients or employees. This disclosure is only made to the extent the personal information is required and is used only for purposes such as the efficient supply of services. Such disclosure requires the receiving person or entity to keep the personal information confidential.

Cassellholme will take reasonable steps to ensure that only employees who need to know or whose duties so require, are granted access to personal information. Cassellholme will use and disclose your personal health information to:

a. treat and care for you;

b. facilitate continuity of care when you are transferred to another facility or hospital;

c. obtain payment for your treatment and care from OHIP, WSIB, private insurer or others;

d. plan, administer and manage our internal operations;

e. conduct risk management and quality improvement activities including resident and client satisfaction surveys

f. teach;

g. compile statistics

h. conduct fundraising initiatives to improve our healthcare services and programs;

i. comply with legal and regulatory requirements, and fulfill other purposes permitted or required by law

Suspected Privacy Breach

A privacy breach is any event where resident, client or employee information is collected, used, or disclosed counter to PHIPA or MFIPPA, Cassellholmes policies, or obligations defined in agreements binding Cassellholme.

The person who identifies a suspected or real breach must:

a. Take immediate steps to prevent any further harm or risk; and
b. Inform the Privacy Officer of the suspected or real breach within one (1) hour of identifying the breach.

It is the responsibility of the Privacy Officer to confirm whether the suspected breach is real and take steps to ensure that no further harm or risk is anticipated. The Privacy Officer will notify residents, clients or SDMs, or employees of the loss, theft, or inappropriate access, use or disclosure of their personal health information as soon as reasonably possible.

ConnectingOntario ClinicalViewer
Where the breach involves a shared technology platform, such as eHealth's Clinical Viewer, the designated Privacy Officer will investigate as outlined in **Appendix A**.

Where a privacy breach has been substantiated, disciplinary action up to and including termination will be considered. Under PHIPA legislation, Cassellholme has mandatory privacy breach reporting requirements to the Information and Privacy Commissioner of Ontario (IPC) as well as to relevant regulatory colleges.

Accuracy of Personal Health Information

When an individual successfully demonstrates the inaccuracy or incompleteness of personal health information; Cassellholme will amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information will be transmitted to third parties having access to the information in question.

ConnectingOntario ClinicalViewer
A resident/client may request access to or make a correction to their care records or other shared records **(Appendix C)** by contacting the Privacy Officer identified herein. Requests for access to information in any shared technology such as the ConnectingOntario ClinicalViewer will be documented in a *Request for Access Log*. In cases where the information being requested has been added by another party, the client/resident will be re-directed to the eHealth Ontario Program Office. Where a correction is made to a health record, the Program Office will be informed and recorded on a *Request for Correction Log.*

Ensuring Safeguards for Personal Health Information

Security safeguards appropriate to the sensitivity of the information will protect personal health information. Security safeguards are used to protect personal health information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Cassellholme protects personal health information regardless of the format in which it is held. The nature of safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage.

The methods of protection will include:

a. physical measures, for example, locked filing cabinets and restricted access to offices
b. organizational measures, for example, policies, training, limiting access on a "need-to-know" basis
c. technological measures, for example, the use of passwords, secure computer networks, encryption, and audits

Cassellholme will make its employees aware of the importance of maintaining the confidentiality of personal health information. As a condition of employment, all new employees/agents (e.g., employee, allied health, volunteer, student, consultant, or contractor) must sign a Confidentiality Agreement with Cassellholme. All employees are required to review a Confidentiality Agreement on an annual basis. This safeguard may also be facilitated though contractual provisions. Care will be used in the disposal or destruction of personal health information, to prevent unauthorized parties from gaining access to the information**.**

Openness About Personal Health Information Policies & Practices

Upon request, residents, clients or employees will be informed of:

a. Cassellholme's privacy policy, which describes Cassellholme's privacy and information practices and is posted on the website and policy portal;
b. Their right to forward an inquiry or make a complaint to Cassellholme's Privacy Officer or to the Information and Privacy Commission; and
c. Their right to obtain access to and/or to request a correction of a record of their personal health information.

Information brochires will be on available in our General Store, posted in the Home and website, and included in the Admissions Process to inform all parties about personal health information policies and practives. For more complex inquiries, Cassellholme will redirect individuals to the Privacy Commission of Ontario or an eHealth Program Office (for inquiries pertaining to ConnectingOntario ClinicalViewer).

Individual Access to Own Personal Health Information

Under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), an individual will be informed of the existence, use, and disclosure of his or her personal health information and will be given access to that information. Note, in certain situations, Cassellholme may not be able to provide access to all the personal health information it holds about an individual. Exceptions to the access requirement will be in accordance with the law. The reasons for denying access will be provided to the individual. Examples may

include information that could reasonably be expected to result in a risk of serious harm or the information is subject to legal privilege.

Application fee

$5 for each FOI request. There is no application fee for a correction request to an individual's personal health information.

Processing time

A written response is required to confirm that an FOI request has been received. Under MFIPPA, Cassellholme has 30 calendar days to process FOI requests except in specific circumstances. An extension may be required if responding within 30 calendar days would interfere with normal business oerations or because finding or compiling the record is very complex, or if more time is needed to confirm whether some of the medical record should be withheld.

Processing fees

Additional fees apply to process a request. The processing fees depend on the nature of the request, including:

a. the type of information being requested (e.g. general records or personal health information);
b. the format to receive the information;
c. the total costs incurred by Cassellholme to produce or copy the information;

A fee estimate will be provided if processing fees will be more than $25. When processing fees are over $100, a deposit may be required. Additional fees include:

a. the cost of every hour of manual search required to locate a record;
b. cost of copies.

If copying a record requires more than 2 hours time or there are more than 50 pages to be copied, the fee provided under the FIPPA Regulation will be charged ($7.50 per 15 minutes search time and 20 cents per page).

Appeal a request

Individuals have the right to appeal any decision about access to records, made by organizations that are covered under Freedom of Information laws.

This includes appealing, if a request for information is denied.

You may file an appeal with the Office of the Information and Privacy Commissioner of Ontario. You must download and complete an Appeal form (or submit a written letter) form to the Information and Privacy Commissioner Registrar within 30 calendar days of the organization giving notice of its decision

Record Retention

a. Any information collected to respond to access and correction requests, inquiries, complaints, and information pertaining to consent directives must be retained for two years after the request was made.
b. Any information created about a resident/client as part of an investigation of Privacy Breaches and/or Security Incidents should be retained for two years after the Privacy Breach has been closed.
c. Audit and monitoring reports that contain PHI created and maintained for compliance purposes should be retained for the longer of thirty years or when PHI is removed from the EHR.
d. Information used for identity provider registration that contains PI should be retained for seven years after last use.
e. System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI should be retained for a minimum of two years.
f. Assurance-related documents should be retained for ten years.

Challenging Compliance with Cassellholme's Privacy Policies & Practices

An individual will be able to address a challenge concerning compliance with this policy. Cassellholme has procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal health information. Cassellholme will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. Cassellholme will investigate all complaints. If a complaint is found to be justified, Cassellholme will take appropriate measures, including, if necessary, amending its policies and practices.

Complaints can be directed to the Privacy Officer at:

(705) 474-4250 Ext. 295, or by e-mail to girouxs@cassellholme.on.ca

Individuals may also make a complaint to the Ontario Information and Privacy Commissioner.

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: (416) 326-3333 or (905) 326-3333
Toll free: 1 (800) 387-0073 (within Ontario)

ConnectingOntario ClinicalViewer
Complaints involving the use of ConnectingOntario ClinicalViewer can be addressed in accordance with **Appendix D**.

Review

HR will review this policy and related procedures on an annual basis, or as required, and will make adjustments as necessary to ensure that it continues to meet the needs of all employees and service providers. .

APPENDIX A

RESPONDING TO A PRIVACY BREACH

1. The person who identifies a suspected or real breach must:
   a. Take immediate steps to prevent any further harm or risk; and
   b. Inform the Privacy Officer of the suspected or real breach within one hour of identifying the breach.
2. The Privacy Officer must confirm whether the suspected breach is real.
3. The Privacy Officer must review the steps to ensure that no further harm or risk is anticipated.
4. The Privacy Officer has authority to take further action to minimize harm or risk up to and including:
   a. Removing the person's access to any paper or electronic copies of medical records, including shared systems;
   b. Retrieving any copies of PHI that were inappropriately collected, used, or disclosed;
   c. Disconnecting systems from the network or Internet;
   d. Requiring support from other members of the clinic to effectively contain the privacy breach; and
   e. Taking any reasonable action to minimize harm or risk to a/the resident(s) or client(s) .
5. Once contained, the Privacy Officer must lead a breach investigation which includes:
   a. Assembling members of the department as required to understand who was responsible for the breach and how it occurred;
   b. Whether the breach was willful or accidental;
   c. Whether other steps could be taken to minimize harm or risk;
   d. The resident/clients that were impacted by the breach; and
   e. Recommendations to prevent further of the same nature breaches.
6. The Privacy Officer must document the breach and investigation using the *Privacy Breach Report Template.*
7. The Privacy Officer must report the breach to eHealth Ontario.
8. The Director of Care or designate must review the recommendations and determine which recommendations should be implemented.
9. The Privacy Officer must develop a plan to implement the approved recommendations and provide status updates to the Director of Care or designate.

APPENDIX B

CONSENT DIRECTIVES

Cassellholme is responsible for complying with the rules relayed in privacy training, including those on collection, use, and disclosure of information in the various information systems used at Cassellholme.

If a resident/client wishes to apply a Consent Directive in the ConnectingOntario system, such requests will be documented on the *Consent Management Request Form* and will be directed to the program office responsible for the shared system (e.g., eHealth Ontario).

Cassellholme or an agent of shall only override a block to collect PHI where the agent or Cassellholme:

1. Obtains the express consent of the resident/client to whom the PHI relates;
2. Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the resident/client to whom the PHI relates and it is not reasonable possible to obtain the consent of the individual in a timely manner; or
3. Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the resident/client to whom the PHI relates or to a group of persons.
4. When a staff member accesses personal health information that is blocked, Cassellholme must confirm that it was appropriate and tell the resident/client that blocked information was accessed.

When resident/client blocks are overridden. The record should include:

1. Resident/client name or other identifiers;
2. Staff Member who overrode the resident/client block;
3. Type of resident/client information that was viewed;
4. Reason for the override; and
5. Date and time that the override occurred.

Notice of Consent Override

Where blocked information was accessed, the Privacy Officer or designate must notify the resident/client of the acesss in and document in the *Consent Directives Log*. He or she muat also notify the Information and Privacy Commissioner of Ontario (IPC) about the occurrence of a consent directive override - only if the override was performed for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the PHI relates or to a group of persons.

Auditing Staff Members' Access to ConnectingOntario ClinicalViewer

The Privacy Officer or designate must get audit reports on the access logs on a monthly basis and follow the guidance provided by the relevant program office for auditing Cassellholme staff members' access to the shared system.

Audit reports will be provided to the manager(s) of the staff members being audited and ask them to confirm their staff members' access. The managers must follow-up with the staff members on any suspicious behavior that they identify and report same to the Privacy Officer or designate.

The Privacy Officer must follow the breach management procedure for any unexplained, suspicious behavior.

APPENDIX C

RECEIVING REQUESTS FOR ACCESS OR CORRECTION RELATED TO SHARED SYSTEMS

If a resident/client requests to view or get a copy of their medical record in ConnectingOntario ClinicalViewer, the Privacy Officer or designate must give the resident/client contact information within 30 days for the eHealth Ontario program office, if the medical record was contributed by another or multiple clinics.

Requests for access or correction will be recorded on the appropriate tracking forms.

APPENDIX D

RESPONDING TO REQUESTS AND INQUIRIES RELATED TO SHARED SYSTEMS

If a person has a question or complaint related to ConnectingOntario ClinicalViewer, the Privacy Officer must:

1. Respond to the question following normal procedures if the answer is known; or
2. Give the resident/client information within 4 days on how to contact the program office responsible for the shared system (e.g., eHealth Ontario) if it relates to the shared system or one or more other health service providers.
3. Record all inquiries and complaints on the *Inquiry and Complaint Log*

REFERENCES:

Personal Health Information Protection Act, 2004, SO 2004, c.3 Sch. A
Information and Privacy Commissioner of Ontario, “Detecting and Deterring Unauthorized Access to Personal Health Information” (Toronto: ON, 2015)
Privacy Policy and Operating Practices Manual - eHealth Ontario, Version: 3.1
Date: March 2017

RELATED POLICIES:
Clinical Services Policy CS-S15: Security Policy –Clinical Viewer
Human Resources Policy 07-10: Conditions of Employment
Human Resources Policy 07-12: Confidentiality
Human Resources Policy 07-13: Confidentiality - Staff Medical Information