Privacy of Client Information Policy and Procedures

Last Updated: June 2026

Gateway
Community Health Centre

Gateway
Community Health Centre

Document Version History

Date	Version	Author/Approval Body	Comments
June 2026	1.0	Senior Leadership Team	Approved Privacy Policy Manual

Document Review Schedule

Document Review Frequency: Annually for one year, then every four years afterwards (4 years)

Next Review Schedule: June 2027

Document Sign-Off

Date	Version	Approval Body
June 8, 2026	1.0	Senior Leadership Team

Gateway Community Health Centre

TABLE OF CONTENTS

PRIVACY POLICY 1

Purpose 1
Policy Statement 1
Principles 1
Forms/Paperwork 5

PRIVACY AND YOUR PERSONAL HEALTH INFORMATION 6

Your Health Record 6
Confidentiality 6
Our Practices 6
Your Choices And Who Decides 6
For More Information Or Complaints 7

ACCESS AND CORRECTION POLICY – RELEASE OF CLIENT INFORMATION 8

Purpose 8
Definitions 8
Procedures 9
Appendix A - Mandatory Disclosures 15

RESTRICTING ACCESS TO MEDICAL RECORDS POLICY AND PROCEDURES 18

Purpose 18
Procedure 18
Implications Of Implementing A Restriction To Access Medical Records 19
Decisions To Implement A Restriction To Access Medical Records 20
Restriction To Access Medical Records Exclusions 20
Identifying A Client Chart Where Access Has Been Restricted 21
"Breaking" The Restriction 21
Auditing And Review Of Restricted Records 22
Breach Of Privacy 22
Attachments 22
Appendix B – Restricting Access To Medical Records Information Brochure 23

SAFEGUARDS FOR CLIENT INFORMATION GUIDELINES 25

Context And Purpose 25
Guidelines 25
Appendix C – Technology Fact Sheet – Disposing Of Your Electronic Media 32

VIRTUAL (VIDEO) CARE POLICY 38

Purpose 38
Policy Statement 38
Procedure 38

PRIVACY BREACH PROTOCOL 42

Purpose And Context 42
Protocol 43
Notifying the IPC/O 44

SHARING INFORMATION WITH POLICE GUIDELINES 45

When can Gateway CHC share information with police? 45
So what can Gateway CHC tell police? 45
General Information 45

Gateway Community Health Centre

PRIVACY POLICY

PURPOSE

Gateway CHC is a health information custodian under the Personal Health Information Protection Act, 2004 (PHIPA). Gateway CHC are accountable and liable for compliance with PHIPA and the protection of health records.

The Privacy Policy acts as the articulation of privacy practices and standards to guide all Staff.

In this privacy policy, Gateway CHC uses the language of "Staff" to capture the commitment that all Gateway CHC employees, physician staff, volunteers, students and vendors and any other agents will abide by this Privacy Policy and to reflect our shared commitment to protecting personal health information.

POLICY STATEMENT

Gateway CHC is committed to client[1] privacy and to protecting the confidentiality of the health information we hold.

PRINCIPLES

- **Principle 1 – Accountable for Personal Health Information**

  Gateway CHC is responsible for any personal health information held.

  The Privacy Officer is accountable for compliance with this Privacy Policy and compliance with PHIPA.

  Our commitment to privacy is demonstrated by adherence to our privacy policies and procedures to protect the personal health information Gateway CHC holds and by educating our staff and any others who collect, use or disclose personal health information on our behalf about their privacy responsibilities.

- **Principle 2 – Identifying Purposes for Collecting Personal Health Information**

  Gateway CHC collects personal health information for purposes related to direct client care, administration and management of our programs and services, client billing, administration and management of the health care system, research, teaching, statistical reporting, quality improvement, accreditation, meeting legal obligations and as otherwise permitted or required by law.

  When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is permitted or required by law, consent will be required before the information can be used for that purpose.

- **Principle 3 – Consent for the Collection, Use and Disclosure of Personal Health Information**

  In general, Gateway CHC requires consent in order to collect, use, or disclose personal health information. However, there are some cases where Gateway CHC may collect, use or disclose personal health information without consent as permitted or required by law.

  Who can consent on behalf of an incapable individual (including very young children) or deceased person, is set out in our "*Access and Correction Policy – Release of Client Information"*.

  ### Express consent

  Should a client wish their other health care providers (outside of their health care providers at Gateway CHC) to have access to the client health record, the client can provide a verbal or written consent to this effect, which will be communicated to the client's primary health care provider. See our "*Access and Correction Policy – Release of Client Information*".

  Should a client wish their lawyer, insurance company, family, employer, landlord or other third-party individuals or agencies (non-health care providers) to have access to their health record, the client must provide verbal or written consent to this effect, which will be communicated in accordance with our "*Access and Correction Policy – Release of Client Information".*

  ### Implied consent (Disclosures to other health care providers for health care purposes) – Circle of Care

[1] We have used the term "client" throughout the policy. It is possible that Gateway CHC holds personal health information about individuals who are not clients of Gateway CHC or who are former clients, and this policy would apply equally to those individuals.

Client information may also be released to a client's other health care providers for health care purposes (within the "circle of care") without the express written or verbal consent of the client as long as it is reasonable in the circumstances to believe that the client wants the information shared with the other health care providers. No client information will be released to other health care providers if a client has stated they do not want the information shared (for instance, by way of the placement of "Restriction of Access" on their health records).

A client's request for treatment constitutes implied consent to use and disclose their personal health information for health care purposes, unless the client expressly instructs otherwise.

Who can be in the "circle of care" includes (among others providing direct client care if authorized by PHIPA).

Within Gateway CHC authorized agents as defined under circle of care include the following:

- Any regulated health professionals, Program Managers, Support and Care Navigators, Medical Secretaries, Certified Dental Assistants, Outreach Workers, Dental Receptionists
- Medical students and residents or nursing or other allied health care students

Outside of Gateway CHC (among others):

- Regulated health professionals in solo practice or group
- Social workers and social service workers in solo practice or group
- Hospitals
- Community Health Centres
- Long-term care homes
- Ambulance/Emergency Medical Services
- Pharmacists
- Laboratories
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care, including as part of other regional or provincial shared care systems to coordinate care for you.

For clarity – the following groups are NOT in the circle of care, and Gateway CHC does not share personal health information about our clients with them relying on implied consent. That does not mean Gateway CHC never discloses to these individuals and groups - but we only do so if we have express consent or if we are otherwise permitted or required by law to disclose:

- Teachers and schools (however, psychologists, social workers, nurses, psychiatrists, speech-language pathologists, occupational therapists, physiotherapists, or audiologists affiliated with schools may be in the circle of care if they are providing health care)
- Children's Aid Society
- Police
- Landlords & Employers
- External unregulated care providers
- Spiritual leaders/healers
- Insurance companies
- Lawyers & Law firms
- Employer's Occupational Health Departments
- Financial Institutions
- Parents, caregivers, family members, neighbors, and friends (NOTE: substitute decision makers stand in the shoes of clients to make decisions and therefore we do not rely on implied consent when sharing information with substitute decision makers)

No Consent

There are certain activities for which consent is not required to collect, use or disclose personal health information. These activities are permitted or required by law.

For example, Gateway CHC do not need consent from clients to (this is not an exhaustive list):

- Plan, administer and manage our internal operations, programs and services.
- Get paid.
- Engage in quality improvement, error management, and risk management activities
- Participate in the analysis, administration and management of the health care system.
- Engage in research (subject to certain rules).
- Teach, train and educate our staff and others.
- Compile statistics for internal or mandatory external reporting

- Respond to legal proceedings.
- Comply with mandatory reporting obligations.

A list of mandatory reporting obligations is found in our "*Access and Correction Policy – Release of Client Information"*.

If staff have questions about using and disclosing personal health information without consent, they can ask the Privacy Officer.

Withholding or Withdrawal of Consent

If consent is sought, a client may choose not to give consent ("withholding consent"). If consent is given, a client may withdraw consent at any time, but the withdrawal cannot be retrospective. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice.

When a client withholds consent, withdraws consent, or places limits on the use of their personal information, they will be informed of any potential implications for service. This may include, for example, limits to treatment or loss of third-party benefits. It is important to communicate these implications clearly to ensure that the person served understands the potential consequences of their decision.

Restricting Access to Medical Records

PHIPA gives clients the opportunity to restrict access to any personal health information or their entire health record by their health care providers within Gateway CHC or by external health care providers. See our "Restricting Access to Medical Records Policy" for details.

If a physician leaves Gateway CHC, their clients will be notified and will have a choice to transfer their health records in accordance with the rules set forth by the College of Physicians and Surgeons of Ontario.

- **Principle 4 – Limiting Collection of Personal Health Information**

Gateway CHC limits the amount and type of personal health information it collects to that which is necessary to fulfill the purposes identified. Information is collected directly from the client, unless the law permits or requires collection from third parties. For example, from time-to-time Gateway CHC may need to collect information from clients' family members or other health care providers and others.

Personal health information may only be collected within the limits of each Staff's role. Staff should not initiate their own projects to collect new personal health information from any source without being authorized by Gateway CHC.

- **Principle 5 – Limiting Use, Disclosure and Retention of Personal Health Information Use**

Personal health information is not used for purposes other than those for which it was collected, except with the consent of the client or as permitted or required by law.

Personal health information may only be used within the limits of each Staff's role. Staff may not read, look at, receive or otherwise use personal health information unless they have a legitimate "need to know" as part of their positions. If a Team Member is in doubt whether an activity to use personal health information is part of their position – they should ask the Privacy Officer. For example, self-directed learning is not allowed (randomly or intentionally looking at health records for self-initiated educational purposes or curiosity) without specific authorization.

Disclosure

Personal health information is not disclosed for purposes other than those for which it was collected, except with the consent of the client or as permitted or required by law.

Personal health information may only be disclosed within the limits of each Staff's role. Staff may not share, talk about, send to or otherwise disclose personal health information to anyone else unless that activity is an authorized part of their position. If a Team Member is in doubt whether an activity to disclose personal health information is part of their position – they should ask the Privacy Officer.

Retention

Health records are retained as required by law and professional regulations and to fulfill our own purposes for collecting personal health information.

Gateway Community Health Centre follows the Canadian Medical Protective Association (CMPA) and College of Physicians and Surgeons of Ontario (CPSO) recommendations to retain health records for at least 10 years from the date of last entry or, in the case of minors, 10 years from the time the client would have reached the age of majority (age 18). In some cases, Gateway CHC keeps records for longer than this minimum period.

Personal health information that is no longer required to fulfill the identified purposes is destroyed, erased, or made

anonymous safely and securely. Please see our "*Safeguards for Client Information Guidelines*".

- **Principle 6 – Accuracy of Personal Health Information**

  Gateway CHC will take reasonable steps to ensure that information we hold is as accurate, complete, and up to date as is necessary to minimize the possibility that inappropriate information may be used to make a decision about a client.

- **Principle 7 – Safeguards for Personal Health Information**

  Gateway CHC has put in place safeguards for the personal health information we hold, which include:

  - Physical safeguards (such as confidential shredding bins, locked filing cabinets and rooms, clean desks);
  - Organizational safeguards (such as permitting access to personal health information by staff on a "need-to-know" basis only); and
  - Technological safeguards (such as the use of passwords, encryption, audits, back-up, secure disposal).

  Gateway CHC take steps to ensure that the personal health information we hold is protected against theft, loss and unauthorized use or disclosure. The details of these safeguards are set out in our "*Safeguards for Client Information Guidelines*".

  Gateway CHC requires anyone who collects, uses or discloses personal health information on our behalf to be aware of the importance of maintaining the confidentiality of personal health information. This is done through the signing of confidentiality agreements, privacy training, and contractual means.

  Care is used in the disposal or destruction of personal health information, to prevent unauthorized parties from gaining access to the information. Gateway CHC will take care if we transfer files to a medical storage company.

- **Principle 8 – Openness about Personal Health Information**

  Information about our policies and practices relating to the management of personal health information are available to the public, including:

  - Contact information for our Privacy Officer, to whom complaints or inquiries can be made;
  - The process for obtaining access to personal health information Gateway CHC holds, and making requests for its correction;
  - A description of the type of personal health information Gateway CHC holds, including a general account of our uses and disclosures; and
  - A description of how a client may make a complaint to Gateway CHC or to the Information and Privacy Commissioner of Ontario.

- **Principle 9 – Client Access to Personal Health Information**

  Clients may make written requests to have access to their records of personal health information, in accordance with our "*Request for Release of Client Information*".

  Gateway CHC will respond to a client's request for access within reasonable timelines and costs to the client, as governed by law. Gateway CHC will take reasonable steps to ensure that the requested information is made available in a format that is understandable.

  Clients have a right to ask for their records to be corrected if they can demonstrate that the records Gateway CHC holds are inaccurate or incomplete in some way for the purposes for which Gateway CHC holds that information. In some cases, instead of making a correction, Gateway CHC may offer a client an opportunity to append a statement of disagreement to their file.

  Please Note:

  In certain situations, Gateway CHC may not be able to provide access to all the personal health information we hold about a client. Exceptions to the right of access requirement will be in accordance with law. 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.

- **Principle 10 – Challenging Compliance with Our Privacy Policies and Practices**

  Any person may ask questions or challenge our compliance with this policy or with PHIPA by contacting our Privacy Officer:

  Mayo Hawco
  41 McClellan St Tweed, ON
  K0K 3J0

Phone: (613)-478-1211

Gateway CHC will receive and respond to complaints or inquiries about our policies and practices relating to the handling of personal health information. Gateway CHC will inform clients who make inquiries or lodge complaints of other available complaint procedures.

Gateway CHC will investigate all complaints. If a complaint is found to be justified, Gateway CHC will take appropriate measures to respond.

The Information and Privacy Commissioner of Ontario oversees our compliance with privacy rules and PHIPA. Any individual can make an inquiry or complaint directly to the Information and Privacy Commissioner of Ontario by writing to or calling:

2 Bloor Street East, Suite 1400 Toronto, Ontario M4W 1A8 Canada
Phone: 1 (800) 387-0073 (or 416-326-3333 in Toronto
Fax: 416-325-9195
www.ipc.on.ca

FORMS/PAPERWORK

Annual Confidentiality Statement

Gateway
Community Health Centre

PRIVACY AND YOUR PERSONAL HEALTH INFORMATION

Gateway CHC is committed to promoting privacy and protecting the confidentiality of the health information we hold about you.

YOUR HEALTH RECORD

Your health record includes information relevant to your health including your date of birth, contact information, health history, family health history, details of your physical and mental health, record of your visits, the care and support you received during those visits, results from tests and procedures, and information from other health care providers.

Your record at Gateway CHC is our property, but the information in your file belongs to you.

With some exceptions, you have the right to access the health information Gateway CHC holds about you. If you request a copy of your record, one will be provided to you. If you wish to view the original record, one of our staff members will be present. If you need a copy of your health record, please contact us in writing at: Gateway CHC, Records Department. In rare situations, you may be denied access to some or all of your record (with any such denial being in accordance with applicable law).

Gateway CHC try to keep your record accurate and up to date. Please let us know if you disagree with what is recorded, and in most cases Gateway CHC will be able to make the change or otherwise we will ask you to write a statement of disagreement and we will attach that statement to your record.

CONFIDENTIALITY

Everyone who works at Gateway CHC is bound by confidentiality. Gateway CHC must protect your information from loss or theft and make sure no one looks at it or does something with your information if they are not involved with your care, or allowed as part of their job. If there is a privacy breach, Gateway CHC will tell you (and we are required by law to tell you).

OUR PRACTICES

Gateway CHC collects, uses and discloses (meaning shares) your health information to:

- Treat and care for you
- Provide appointment or preventative care reminders to you and/or send client surveys to you
- Update you of upcoming events, activities and program.
- Coordinate your care with your other health care providers including in regional and provincial groups like Ontario Health Team and integrated models of care
- Deliver and evaluate our programs
- Plan, administer and manage our internal operations.
- Be paid or process, monitor, verify or reimburse claims for payment
- Conduct risk management, error management and quality improvement activities
- Educate our staff and students
- Dispose of your information
- Seek your permission (or permission of a substitute decision maker) where appropriate
- Conduct research (subject to certain rules)
- Compile statistics
- Allow for the analysis, administration and management of the health system
- Comply with legal and regulatory requirements
- Fulfill other purposes permitted or required by law

Our collection, use and disclosure (sharing) of your personal health information is done as allowed by Ontario law.

YOUR CHOICES AND WHO DECIDES

You have a right to make choices and control how your health information is collected, used, and disclosed, subject to some limits.

You may make your own decisions if you are “capable”. Your Primary Care Provider will decide if you are capable based on a test the law sets out. You may be capable of making some decisions and not others. If you are not capable – you will have a substitute decision-maker who will make your information decisions for you. Who can act as a substitute decision-maker and what they have to do is also set out in law.

If you are under the age of 16, there are some additional rules about who can make decisions about your health information. If you are capable of making your own decisions, you may be able to decide how your health information is collected, used, and shared. In some situations, your parent or guardian may also have the right to make decisions about your health information. Your health care provider can explain which rules apply to you.

Gateway CHC assumes that when you come to have health care from us, you have given us your permission (your consent) to use your information, unless you tell us otherwise. Gateway CHC may also collect, use and share your health information in order to talk with other health care providers about your care unless you tell us you do not want us to.

You have the right to ask that Gateway CHC not share some or all of your health record with one or more of our staff, or ask us not to share your health record with one or more of your external health care providers (such as a specialist). This is known as asking to restrict access to your medical records.

There are other cases where Gateway CHC is not allowed to assume we have your permission to share information. Gateway CHC may need permission to communicate with any family members or friends with whom you would like us to share information about your health (unless someone is your substitute decision-maker). For example, Gateway CHC will also need your permission to give your health information to your boss, partner, parent, child, to an insurance company or a school. If you have questions, we can explain this to you.

When Gateway CHC requires and asks for your permission, you may choose to say no. If you say yes, you may change your mind at any time. Once you say no, Gateway CHC will no longer share your information unless you say so. Your choice to say no may be subject to some limits.

BUT there are cases where Gateway CHC may collect, use or share your health information without your permission, as permitted or required by law. For example, Gateway CHC does not need your permission to use your information for billing, risk management or error management, quality improvement purposes. Gateway CHC also do not need your permission to share your health information to keep you or someone else safe (it’s called to eliminate or reduce a significant risk of serious bodily harm); or to meet reporting obligations under other laws such as for child protection or transportation safety (driving a vehicle).

FOR MORE INFORMATION OR COMPLAINTS

If you would like a copy of our Privacy Policy, please visit Gateway CHC’s website www.gatewaychc.org.

Gateway CHC encourages you to contact us with any questions or concerns you might have about our privacy practices. You can reach our Privacy Officer at Gateway CHC.

If, after contacting us, you feel that your concerns have not been addressed to your satisfaction, you have the right to complain to the Information and Privacy Commissioner of Ontario. The Commissioner can be reached at:

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400 Toronto, Ontario M4W 1A8
1-800-387-0073
1-416-325-9195 (fax)
www.ipc.on.ca

Gateway Community Health Centre

ACCESS AND CORRECTION POLICY – RELEASE OF CLIENT INFORMATION

PURPOSE

This Policy is part of Gateway CHC's Privacy Policy

Gateway CHC is a health information custodian and owns health records of its clients. However, the information in the health record belongs to the client and the client has a right of access to that information and the right to direct Gateway CHC to share that information or not share that information with others, subject to some exceptions.

This policy addresses five activities:

- Client[2] requests for access to their own health records ("**access**")
- Client requests to correct their own health records ("**correction**")
- Requests to share information with other organizations or health care providers with express consent or implied consent ("**circle of care**")
- Requests to transfer client files to a new health care provider or organization ("**transfer**")
- Third party requests for a copy of a client's health record ("**release of information**") such as from lawyers, insurance companies and police

DEFINITIONS

Consent and "Authorized Persons"

When consent is required under this policy, the following authorized persons may give consent:

1. **The client, if the client is capable**
   a. **Please note for capable clients under the age of 16:** If a client is capable and under the age 16, the client may consent AND the client's parent or person who has lawful custody may also consent. BUT the parent or person with lawful custody may not consent if the information to be disclosed relates to "treatment" (as defined under the *Health Care Consent Act, 1996)* about which the child has made their own decision or "counseling" (as defined under the *Child and Family Services Act)* about which the child participated on their own.

   That means if a child consented to the care on their own, a parent cannot consent to the release of that information on behalf of the child. And if there is a disagreement between a capable child and the parent about the release of information, the capable child's wishes prevail. If staff have questions about consent for children, please ask the Privacy Officer.

2. **A substitute decision-maker, if the client is incapable.**

   Please refer to section 26 of PHIPA which lists the hierarchy of individuals/agencies that can act as substitute decision-makers:

   - The individual's guardian of the person or guardian of property, if the consent relates to the guardian's authority to make a decision on behalf of the individual (you must see a copy of the documentation).
   - The individual's power of attorney for personal care or attorney for property, if the consent relates to the attorney's authority to make a decision on behalf of the individual (you must see a copy of the documentation).
   - The individual's representative appointed by the Consent and Capacity Board, if the representative has authority to give the consent (you must see a copy of the documentation).
   - The individual's spouse or partner.
   - A child or parent of the individual, or a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent [Note: This paragraph does not include a parent who has only a right of access to the individual. If a children's aid society or other person is lawfully entitled to consent in the place of the parent, this paragraph does not include the parent.]
   - A parent of the individual with only a right of access to the individual.
   - A brother or sister of the individual.

[2] Gateway CHC has used the term "client" throughout the policy. It is possible that Gateway CHC holds personal health information about individuals who are not clients or who are former clients and this policy applies in those cases as well. Requests for access may also come from a client's substitute decision-maker or "authorized person" as identification in this policy.

- Any other relative of the individual.

3. The estate trustee, in the case of a deceased client

a. Gateway CHC verify the identity of the estate trustee by reviewing a will or the notarized "Certificate of Appointment of Estate Trustee with a Will" or "Certificate of Appointment of Estate Trustee without a Will". A copy of this documentation must be kept. If the deceased client does not have an estate trustee, consent can be obtained from the person who has assumed responsibility for the administration of the deceased person's estate – if documented in writing. If in doubt, ask the Privacy Officer.

When consent is required, clients may withhold or withdraw consent. If clients decide to withhold or withdraw consent, that decision will be documented in their health record.

If the client requests restrictions on the use of and disclosure of their health record, then the client's primary health care provider meets with the client to discuss what is restricted and how this can be done. The primary health care provider needs to explain the repercussions of making this choice. See the **Restricting Access to Medical Records Policy and Procedures** for information about how clients may choose not to share information with other health care providers or organizations.

Copies versus Originals

Originals of health records are not given to clients or released to other health care providers or third parties (except in rare situations if originals are required by law). In most situations, only copies are released. Clients may ask to view original documents as set out below.

PROCEDURES

Please note, front line administrative staff will not dispense any client information themselves, unless directed to do so by the client's primary care provider who is the author of the record or the Privacy Officer.

1. Client Access to Information

With limited exceptions, Gateway CHC is required by law to give clients[3] access to their records of personal health information within 30 days (subject to a time extension of up to an additional 30 days if necessary and with notice to the person making the request).

a. Informal Client Access

From time to time, Gateway CHC will agree to give part of a client's health record to a client directly without engaging in a formal request for access under this policy. For example, sometimes a client needs a list of medications or a copy of particular test results. The primary health care provider decides whether to release this information informally and who can do that on their behalf (e.g. another clinician, front line or administrative staff). The provider will send a Release of Information task to secretary instructing what note(s) to print and to release to the client. Also, it is good practice to stamp "Client Copy" to alert that a document has been released to the client directly (this protects us in case of client losing information).

b. Written Requests

i. Client requests for their own information should be made in writing. Staff must have clients fill out the "Request for Personal Health Information" form.

ii. If a request for access is made to the health care provider, they should direct the client to Gateway CHC's usual process for release of records. Gateway CHC may assist the client with locating the desired information/document in the record. Because records may be difficult to read and interpret and may mislead or alarm a client, clients will be encouraged to review the records with their primary health care provider (or delegate) so the information can be explained.

iii. If a client wishes to read the original health record, someone must be present to ensure the records are not altered or removed. Clients may not make notes on the original health record or remove originals from the health record or otherwise alter their health records. If a client requests a copy of a health record, copies may be given.

iv. The original of the written request for access shall be placed with the client's records and must contain the following:
- A description of what information is requested

[3] Clients and "authorized persons" as defined in this policy may be given access to health records.

- Information sufficient to show that the person making the request for access is the client or other authorized person
- The signature of the client or other authorized person and a witness to the signature
- The date the written request was signed

v. A notation shall be made in the record stating:

- What information or records were disclosed
- When the information or records were disclosed
- By whom the information or records were disclosed

vi. Clients will be asked to provide a signature on a form indicating the date and time the record was picked up.

2. Telephone Requests

Only limited information should be given out over the telephone to a client, as it may not be possible to verify that client's identity. **See the "Safeguards for Client Information Guidelines".**

3. Walk-in Requests

A signed consent is required for access to a client's record. Clients will be requested to return at a later date to pick up authorized information.

4. Denying Client Access to Health Records

In certain situations, Gateway CHC may choose not to provide a client with access to all or part of a health record. Exceptions to the right of access requirement must be in accordance with law and professional standards. Reasons to deny access to a health record (or part of a health record) may include:

- The information is subject to a legal privilege that restricts disclosure to the individual (i.e. court order)
- The information was collected or created primarily in anticipation of or for use in a proceeding (and that proceeding and any appeals have not been concluded)
- The information was collected or created in the course of an inspection, investigation or similar procedure authorized by law or undertaken for the purpose of the detection, monitoring or prevention of a person's receiving or attempting to receive a benefit to which the person is not entitled under law (Ongoing investigations or proceedings).
- If granting access could reasonably be expected to:
  - Result in a risk of serious harm to the treatment or recovery of the individual or a risk of serious bodily harm to the individual or another person
  - Lead to the identification of a person who was required by law to provide information in the record
  - Lead to the identification of a person who provided information explicitly or implicitly in confidence (if it is appropriate to keep that source confidential)

Clients must be told if they are being denied access to their own health records. In some situations, Gateway CHC may advise a client that we can neither confirm nor deny the existence of a record. Gateway CHC gets legal advice in such cases. If denied information, clients have a right to complain to the Information and Privacy Commissioner of Ontario and must be told of this right and how to reach the Commissioner's office.

5. Correction of Health Records

A clinician may edit or correct any note they author.

If an error was due to an administrative error (such as a client's record is misfiled in another client's record or there is a data entry error) and is noticed by administrative staff, that error may be fixed by the administrative staff so long as the error is identified before the health care provider had the opportunity to act on it and before anyone else received it externally. If the entry or record has been in the chart for more than a day in error, staff must notify the primary health care provider and any other clinical staff involved in that client's care that it is in the chart in error. If any action was taken based on the false information by any staff member, the erroneous information must be scanned into the chart and attached to a note indicating the error and the deletion. In such cases, Gateway CHC may need to seek legal advice.

Requests for Correction

Gateway CHC has an obligation to correct personal health information if it is inaccurate or incomplete for the purposes it is to be used or disclosed by Gateway CHC.

Clients may request that their health information be corrected if it is inaccurate or incomplete. Such requests must be made in writing and must explain what information is to be corrected and why.

Gateway CHC must respond to requests for correction within 30 days (or seek an extension). Corrections are made

in the following ways:

- Striking out the incorrect information in a manner that does not obliterate the record or
- If striking out is not possible:
  - Labelling the information as incorrect, severing it from the record, and storing it separately with a link to the record that enables us to trace the incorrect information, or
  - Ensuring there is a practical system to inform anyone who sees the record or receives a copy that the information is incorrect and directing that person to the correct information.

The record will not be corrected if:

- The record was not originally created by Gateway CHC and we do not have the knowledge, expertise or authority to correct the record,
- It is not inaccurate or incomplete,
- The change requested does not have to do with the purpose for which we keep the record or use or disclose it, or
- The record consists of a professional opinion which was made in good faith.

Where Gateway CHC chooses not to correct a record, the client must be informed in writing. The client will have the choice to submit a statement of disagreement. If the client submits such a statement, it will be scanned onto the health record and released any time the information that was asked to be corrected is released.

Where Gateway CHC chooses not to correct a record, clients have a right to complain to the Information and Privacy Commissioner of Ontario.

6. Release of Information to Health Care Providers

Express Consent

Should a client wish their other health care providers working externally to Gateway CHC to have access to the client health record, the client can provide a written statement of consent to this effect (release of information):

The following is the process for releasing health records to a third-party health care provider or organization relying on a client's express consent: Record the date of the request in the health record:

i. Advise the client's primary health care provider of the request

ii. If release of information to the third-party organization is authorized by the primary health care provider:

a. Select and photocopy/print requested specific information

b. Do not photocopy/print the entire health record unless required

c. Send out/mail out requested information

d. Scan the letter of request, client's consent, and a copy of the covering letter and save in the client's health record

e. Costs (if applicable) associated with release of information will be invoiced by Gateway CHC

iii. If the request is incomplete, unclear or contains an invalid consent or is otherwise not authorized by the primary health care provider:

a. Inform the client who made the request of the problem in writing (or in person or by phone as appropriate), such as:

- The request is not sufficient to identify the client
- The request is unclear or unspecific
- The request does not have the required consent

b. Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

Implied Consent – Circle of Care

Gateway CHC may also release information to a client's other health care providers and organizations for health care purposes (within the "circle of care") without the express written consent of the client as long as it is reasonable in the circumstances to believe that the client wants the information shared with other health care providers and organizations. However, no information will be released to other health care providers and organizations if a client

has stated they do not want the information shared.

The following is the process for releasing health records to a third-party health care provider relying on a client's implied consent:

i. **Record the date of the request in the health record**
ii. **Advise the client's health care provider of the request**
iii. **If release of information to the third-party health care provider is authorized by the health care provider:**
    a. Select and photocopy/print requested specific information
    b. Do not photocopy/print the entire health record unless required
    c. Send out/ mail out requested information
    d. Record the verbal request for information
    e. Costs associated with release of information will be invoiced by Gateway CHC
iv. If the request is incomplete, unclear or Gateway CHC have been advised by the client not to disclose relying on implied consent, or the request is otherwise not authorized by the health care provider:
    a. Inform the client who made the request of the problem in writing (or in person or by phone as appropriate), such as:
        - The request is not sufficient to identify the client
        - The request is unclear or unspecific
        - The request does not have the required consent
        - Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

7. Transfer of Client Records to a New Health Care Provider

If moving to another primary care provider and wishes Gateway CHC files to be transferred, the client will need to see their new physician or primary health care provider and sign a consent form with them for the release of information. If this is not possible, the client may sign a copy of the Release of Health Information form.

Clinical health records are transferred only with a written request signed by the client (or client's authorized person). A verbal request is not sufficient to transfer health records.

Originals of records are never sent as they are the property of Gateway CHC and must remain accessible to Gateway CHC staff.

When a Release of Health Information form comes in to transfer client records, staff will prepare the client's health care record, scan the transfer request to the appropriate primary health care provider's inbox. The primary health care provider is responsible for responding to the request as soon as possible by either:

- Writing a summary of the client's pertinent health history, or
- Directing staff regarding the relevant information to copy from the client's health care record.

A copy of the Request of Health Information form should be filed in the client's health care record with the date of transfer marked on this form.

When mailing the file, the envelope will be to the attention of the provider and marked "Confidential".

When the file is requested on a USB key for transferring, the USB key will be encrypted. The password of the USB key will be sent on a separate mail or the recipient will be notified of the password.

Upon the completion of transferring client records to the new health care provider, Gateway CHC will inactivate the client's chart.

8. Third Party Requests for Release of Information (to Non-Healthcare Providers)

Should a client wish their lawyer, insurance company, employer, landlord or other such persons or agencies to have access to the client health record, the client must provide a written statement of consent to this effect, which will be directed to the client's primary health care provider. We will not process verbal third-party requests for release of information to anyone who is not a health care provider. These requests must be in writing. No information will be released without the express consent from the client or the authorized person (unless permitted or required by law. Third party requests not accompanied by appropriate consent will be returned with an official letter, outlining proper and complete consent requirements.

Any third-party request for release of information shall include:

- The name, address and telephone number of person/agency requesting the information
- The full name, address and date of birth of the person about whom the information relates
- A specific description about the type and amount of information to be released
- A consent for release of information form signed by the client (or client's authorized person)

The following is the process for releasing health records to a third party with consent of the individual client:

- **Record the date of the request in the health record**
- **Advise the client's primary health care provider of the request**
- **If release of information to the third party is authorized by the primary health care provider:**
  - Select and photocopy/print requested specific information
  - Do not photocopy/print the entire health record unless required
  - Send out/mail out requested information
  - Scan the letter of request, consent, and a copy of the covering letter and save in the client's health record
  - Costs associated with release of information will be invoiced by Gateway CHC
- **If the request is incomplete, unclear or contains an invalid consent or is otherwise not authorized by the primary health care provider:**
  - Inform requester of the problem in writing (or in person or by phone as appropriate), such as:
    - The request is not sufficient to identify the client
    - The request is unclear or unspecific
    - The request does not have the required consent
    - The date the client's consent was signed is not recent; while legally still accurate, you may ask why it has taken a length of time for it to be provided.
  - Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

9. Permitted or Mandatory Release of Information

Gateway CHC may release personal health information to a third party if "permitted or required by law". A list of mandatory disclosures is included at the end of this policy.

Any time a mandatory disclosure is considered, the client's primary health care provider (and as necessary the Privacy Officer) is to be informed PRIOR to reporting. Legal advice may be sought.

Police/OPP/RCMP

There is a natural tendency to want to cooperate with the police and assist them in their investigations. However, this must be balanced against clients' right to privacy and the right to confidentiality of their personal health information.

The fact that a client is suspected of being a victim of a crime or suspected of having committed a crime is not a recognized reason for breaching the client's right to confidentiality. However, there is a recognized exception ("discretion to warn") to client confidentiality where there is a significant risk of serious bodily harm to someone (either the client or someone else) **and if it is genuinely believed that disclosing information to police could eliminate or reduce that risk.**

Otherwise, personal health information will only be released to police upon the presentation of one of the following documents:

- **A consent for release of information form signed by the client or authorized person**
- **A valid court order (or other legal document) requiring the release of information to the police**
- **A coroner's writ requiring the release of information to the police**

Each document must be reviewed carefully before information may be disclosed to police (to ensure the disclosure

is **permitted or required** by law). This review should be done by appropriate staff, such as the client's primary health care provider and/or the Privacy Officer before any information is released. The documentation from the client, police, court or coroner will be scanned into the chart. Legal advice should be sought as necessary.

Children's Aid Society (CAS)

Health professionals have a mandatory duty to report a "child in need of protection" to the CAS under the *Child, Youth, and Family Services Act*. Information may be sent to the CAS to explain the reason for the report.

Where the CAS is the legal guardian of a child, the CAS should be treated as any other parent or guardian would be in response to a request for access to or disclosure of the health records.

Any documentation from CAS claiming authority to release information to the CAS must be reviewed carefully before information may be disclosed (for the section of the legislation giving the legal authority that the release of information is **permitted or required** by law). This review should be done by the client's primary health care provider and/or the Privacy Officer before any information is released. The documentation from CAS will be scanned into the chart. Seek legal advice as appropriate.

Regulatory Colleges

Under the *Regulated Health Professions Act, 1991* and other health profession specific legislation, regulatory Colleges may have the authority to review client records as part of investigations or quality assurance practices. Any documentation from a regulatory College claiming legal authority to release information to the College must be reviewed carefully before information may be disclosed (for the section of the legislation giving the legal authority that the release of information is **permitted or required** by law). This review should be done by the client's primary health care provider and/or the Privacy Officer before any information is released. The documentation from the regulatory College will be scanned into the chart.

Other Authorities

Certain legislation gives government agencies and others authority to review client records (such as immigration, the Ministry of Health and Long-Term Care, workplace safety and insurance and others). Any documentation from an agency claiming legal authority to release information to the agency must be reviewed carefully before information may be disclosed (for the section of the legislation giving the legal authority that the release of information is **permitted or required** by law). This review should be done by the client's primary health care provider and/or the Privacy Officer before any information is released. The documentation from the agency will be scanned into the chart.

Lawyers

Most lawyers' letters require client consent for the release of information to a lawyer. **NEVER release information to a lawyer without client consent unless you have some other documentation to state that Gateway CHC is required by law to disclose the information.** Any documentation from a lawyer claiming legal authority to release information to the lawyer must be reviewed carefully before information may be disclosed (in most cases the lawyer is asking for the record – not advising Gateway CHC that it is required by law to release the record). This review should be done by the client's primary health care provider and/or the Privacy Officer before any information is released. The documentation from the lawyer will be scanned into the chart.

Communicable Disease

The *Health Protection and Promotion Act* requires certain health care providers and organizations to report all communicable diseases to the local Public Health Unit. Reporting is done by the client's physician or nurse practitioner or delegate as soon as possible after the diagnosis is made.

Gateway
Community Health Centre

APPENDIX A - MANDATORY DISCLOSURES

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
Child in need of protection	Information about a "child in need of protection" (e.g., suffering, abuse or neglect). Only information that is reasonably necessary to make the report should be shared. Ongoing information sharing after the report has been made should only be done with express consent or as permitted or required by law, such as a court order for the client health record.	Any person, including a person who performs professional or official duties with children	Relevant Children's Aid Society	Child and Family Services Act, ss. 72(1) and 72(2).
Sexual abuse	Where there are reasonable grounds to believe a health care professional has sexually abused a client, details of the allegation, name of the health care professional and name of the allegedly abused client. The client's name can only be provided with consent. You must include your name as the individual filing the report.	All regulated health providers	Registrar of the suspected healthcare professional's regulatory College	Regulated Health Professions Act Schedule 2, ss. 85.1, 85.3. See also, Social Work and Social Service Work Act, ss. 43 and 44.
Safe driving	Name, address and condition of a person over the age of 16 who has a condition that may make it unsafe for them to drive.	Physicians, registered nurses in the extended class, and optometrists	Registrar of Motor Vehicles	Highway Traffic Act, s. 203(1).
Air crew	Information about flight crew members, air traffic controllers or other aviation license holders who have a condition that may impact their ability to perform their job in a safe manner, likely to constitute a hazard to aviation safety.	Physicians and optometrists	Medical advisor designated by the Minister of Transport	Aeronautics Act, s. 6.5(1).
Seaman	Information about a seaman.	Physicians, surgeons, hospital official	If requested by the seaman's employer	Merchant Seamen Compensation Act, s. 48.
Railway workers	Information about clients who work in the railway industry who have a condition that may put the safety of rail travel at risk.	Physicians and optometrists	A railway designated organization	Railway Safety Act, s. 35(2).
Fraud	Information about health care fraud, including an ineligible person receiving or attempting to receive an insured service; an ineligible person obtaining or attempting to obtain reimbursement by OHIP for money paid for an insured service; or an ineligible person, in an application, return or statement made to OHIP or the General Manager, giving false information regarding his or her residency.	Physicians and registered nurses in the extended class, podiatrist, chiropractor, midwife, optometrist, dentist, dental surgeon, operator of a physiotherapy facility, hospital, facility whose primary function is the provision of insured services, laboratory, specimen collection Centre	General Manager of OHIP	Health Insurance Act, s. 43.1(1) and Health Fraud Regulation, s. 1.

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
Queue jumping	Information about an individual offering to pay, confer, charge or accept a benefit in exchange for improved access to health care.	Physicians, registered nurses in the extended class, podiatrists, midwives, optometrists, dentists, dental surgeons, licensees under the Independent Health Facilities Act, hospital, or private hospital	General Manager of OHIP	Commitment to the Future of Medicare Act, ss. 17(1) and 17(2) and General Regulation, s. 7(1).
Reportable or communicable disease	Information about a client who has or may have either a "reportable" or "communicable" disease. The report should include the client's name and address in full, date of birth in full, sex, and date of onset of symptoms.	Physicians and registered nurses in the extended class and hospital, children's residence, childcare centre, home for special care, long-term care home, psychiatric facility, and others	Medical Officer of Health of the appropriate health unit	Health Protection and Promotion Act, s. 26 and Reporting Regulation, s. 1(1).
Communicable disease	Name and address of a client receiving care and treatment for a communicable disease but who is neglecting or refusing to comply with the treatment regime.	Physicians and registered nurses in the extended class	Medical Officer of Health	Health Protection and Promotion Act, s. 34(1).
Rabies	Animal bites or animal contact that may result in humans contracting rabies	Physicians and registered nurses in the extended class, and other persons with information about animal bites	Medical Officer of Health	Health Protection and Promotion Act and Communicable Diseases Regulation, s. 2(1).
Immunizations	Instances of adverse reactions to immunizations.	Physicians, nurses, and pharmacists	Medical Officer of Health of the appropriate health unit	Health Protection and Promotion Act, s. 38(3).
Birth	Births.	Physicians and midwives, or nurses if neither of the above are present at birth	Registrar General	Vital Statistics Act, ss. 8, 9.1 and General Regulation, ss. 1(1) and 19(1).
Death	Facts surrounding the death of an individual in prescribed circumstances, e.g., violence, negligence or malpractice. Information requested for the purpose of an investigation.	Any person with information about the circumstances of the death	Coroner or designated Police Officer	Coroners Act, s. 10(1).
Death	Deaths.	Physicians and registered nurses in the extended class	Registrar General	Vital Statistics Act, s. 21(1) and General Regulation, ss. 35(2) and 35(3).
Occupational assessments	Reasonable conclusions of an occupational illness	Physicians who conduct medical examinations or supervise clinical tests for workplace safety	The worker's employer, the joint health and safety committee and the Provincial Organization	Health Protection and Promotion Act, s. 30. Occupational Health and Safety Act and the Designated Substances Regulation, ss. 29(2), 29(3), 29(6) and 29(7).

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
WSIB	Information requested by the WSIB about workers claiming benefits under the Workplace Safety and Insurance Act.	All health care providers	Workplace Safety and Insurance Board (WSIB)	Workplace Safety and Insurance Act, s. 37(1).
Self-report of offence	Information if you yourself are found guilty of an offence, to include: your name; the nature and description of the offence; the date you were found guilty of the offence; the name and location of the court where you were found guilty of the offence; and the status of any appeals.	All regulated health care providers	Registrar of your regulatory College	Regulated Health Professions Act, Schedule 2, ss. 85.6.1(1) – (3).
Self-report of professional negligence or malpractice	Information if you yourself are found guilty of professional negligence or malpractice, to include: your name; the nature and description of the finding; the date the finding was made; and the status of any appeals.	All regulated health care providers	Registrar of your regulatory College	Regulated Health Professions Act, Schedule 2, ss. 85.6.2(1) – (3).
Employer report if end of professional relationship	A written report, within 30 days, regarding revocation, suspension, termination or dissolution of a health care professional's privileges, employment or practice for reasons of professional misconduct, incapacity or incompetence.	Employer or person who offers privileges to a member	Registrar of the college of the regulated healthcare professional	Regulated Health Professions Act, Schedule 2, s. 85.5(1),85.5(3).

RESTRICTING ACCESS TO MEDICAL RECORDS POLICY AND PROCEDURES

PURPOSE

This policy is part of the Privacy Policy.

It applies to all Gateway CHC staff, providers, students, volunteers (including Board members), and vendors. ("Staff")

Ontario's health privacy law, the Personal Health Information Protection Act ("PHIPA"), provides individuals[4] with the right to make choices about, and control how, their personal health information ("PHI")[5] is collected, used, and disclosed.

PHIPA gives clients the opportunity to restrict access to any or their entire PHI by one or more Staff or by external health care providers. The restricting access to one's personal health information provisions of PHIPA are found in sections 37(1)(a), 38(1)(a), and 50(1)(e). The provisions do not extend to other uses or disclosures that are permitted or required under PHIPA or other legislation.

This policy will help our Staff understand and fulfill their role when addressing restricting access to medical records requests and providing care to clients who have implemented these restrictions. Restricting access may affect clinical practice for Gateway CHC because access to information about clients may be restricted, and physicians and interprofessional health care providers may be asked not to share PHI with other health care providers inside or outside of Gateway CHC.

PROCEDURE

Requests for Restricting Access to Medical Records

Any current or former client[6] may request restrictions on access to their medical records, or restrictions on sharing of all or some of their PHI by one or more Staff or by external health care providers. In addition, the client may request partial restriction such as certain notes. Clients can instruct Gateway CHC or their provider not to use or share specified information for health care purposes, including within interdisciplinary teams or externally to others in their circle of care. However, clients cannot restrict uses or disclosures permitted or required by PHIPA, such as when disclosure is necessary to prevent serious harm. Any disclosures and related circumstances are documented in the client's chart, and the client may be informed of the disclosure if appropriate.

When clients ask about restricting access to their records, it is important for Staff to address their concerns about the confidentiality of their PHI. Clients may want something like this when they use words such as "restrict," "limit," "exclude," "shield," or "block," when talking about their PHI. For example, if they ask their health care provider or other Staff Member:

- Not to tell their specialist that they are being treated at Gateway CHC
- Do I have to share my information with that person?
- To exclude certain clinical staff from seeing their information
- To "shield" their information
- To "restrict" their health record
- Not to let their family members or neighbours who work with Gateway CHC look at their health record

Clients may initiate the process for restriction to access medical records by speaking with their primary care provider. The process for request for a restriction to access medical records is as follows:

- A client's verbal request to restrict their records is entered into their chart by their provider by another staff member. Clients are informed that they should make the request in writing and are given the request form to complete
- Clients must submit their requests for a restriction to access medical records in writing
- Clients will be asked to complete a Request Form for Restricting Access to Medical Records
- The completed form must be submitted to the CEO for approval
- Once the request is approved, the Manager of Primary Care will send the original copy to scan to the client's chart.

[4] It is possible that Gateway CHC hold PHI about individuals who are not clients or who are former clients, and the Restricting Access to Medical Records policy would apply equally to those individuals.
[5] "PHI" is broadly defined under PHIPA. In our context it will mainly relate to a client's health record and Gateway CHC has used "health record" interchangeably with PHI throughout the policy. It is possible that Gateway CHC holds other PHI about an individual outside the health record and the Restricting Access to Medical Records policy would apply equally to that information, wherever it resides.
[6] An individual's substitute decision-maker may also request a restriction to access medical records and such requests are processed in the same manner

- The Manager of Primary Care will implement the restriction.
- See below the Implication of Implementing a Restriction to Access Medical Records

The "Restricting Access to Medical Records Information" brochure should be given to clients who want more information. This brochure discusses the purpose, implications, and limitations of implementing a restriction to access medical records.

Restricting access to medical records requests can vary considerably. A client may request that:

- Only some of the documents in their health record be restricted
- All of their health record be restricted
- Only one Staff member be restricted from accessing PHI
- Several Staff be restricted from accessing PHI
- One or more external health care providers not be given their PHI – The client's provider or designate will enter a global message to alert other EMR users about the request.

Although PHIPA does not require that we restrict documentation that does not yet exist, in practice, refusing to restrict future documents may result in frequent restricting access to medical records requests from a client. For this reason, Gateway CHC will, where appropriate and if requested, restrict documents as they are created. An example might be where a client requests a future restriction because one of their family members (or former spouse or partner) is a staff member.

When clients request Restriction to Access Medical Records, it often means they have concerns about their PHI and how it is being used and/or disclosed. Clients should be reminded that:

- Gateway CHC takes privacy seriously and keep all PHI confidential and secure
- PHI is only accessed by staff on a need-to-know basis
- Gateway CHC conducts privacy audits to ensure compliance with the need-to-know policy
- Where PHI is accessed without authorization, appropriate steps will be taken to prevent a reoccurrence and there would be disciplinary consequences
- PHI is disclosed only to external health care providers with whom the client wants their PHI shared (unless the disclosure is otherwise permitted or required under PHIPA without consent, or by another law)

Sometimes a client requests restriction on who is able to access their medical records when the restriction is not necessary to resolve the client's concern. For example, restricting access is not necessary to restrict the sharing of PHI with non-health care providers (e.g., family, employers, insurers) because Gateway CHC needs the client's express consent (either in writing or if verbal, as documented by us) to share information with such recipients (unless, for example, a family member acts as the client's substitute decision-maker). If a client does not want us to share information with non-health care providers – Gateway CHC will not do so unless there is legal authority to do so.

As another example, if a client disagrees with the information in their health records, they can ask for a correction and/or append a statement of disagreement to the record. See the *Access and Correction Policy*. For that reason, they may not need a restriction to access medical records to solve their concerns about the accuracy of the information in their health record.

Chart Locking & Masking

There are 4 chart locking options:

1. Locking Full EMR (omits patient module and appointments)
2. Masking a Chart Note or Individual Item
3. Masking Medication
4. Masking Appointment Information

Charts can be made private (with the exception of patient demographics) by applying the appropriate privacy settings with the EMR system.

Demographic information (Name, OHIP #, DOB) cannot be masked & must be collected for insurance & identity purposes. (For more information please refer to the Personal Health Information Protection Act, 2004.)

Unlocking or modifying a restriction should be completed by the individual who originally applied the restriction, if possible. If that individual is no longer available (e.g. no longer works at Gateway CHC,) the Privacy Officer or designate must authorize the removal or modification of the restriction. Technical support from the organization's electronic medical record (EMR) vendor will be obtained where required.

Implications of Implementing a Restriction to Access Medical Records

If a client chooses to move forward with a Restriction to Access Medical Records request, it is important that they understand the possible implications of the request. There may be implications and risks to the client and to their care. The client's

Physician, or a member of the care team, should discuss implications and risks with the client. Examples may include:

- The client not receiving the best possible service because health care providers may not have access to PHI that they need in order to provide the best possible care in a timely manner.
- The client may have to undergo duplicate tests, procedures and/or health history questions, as applicable, if existing information is unavailable.
- Gateway CHC uses an interdisciplinary team approach to providing care. Although each Restriction to Access Medical Records request is considered on a case-by-case basis, generally, a client's choice to implement a restriction should not prevent a team from providing care as per their standards of practice.
- There may be circumstances where the interdisciplinary team providing health care cannot provide care in a manner that meets their professional standards of practice if they do not have sufficient information. Staff members may have to assess whether they can continue to provide care to a client if there is insufficient information. However, the decision to discontinue care to a client is a significant one and would only be made after thorough consideration of all the relevant information. All staff will try to maximize client choice about how their PHI is used and disclosed while at the same time allowing all members of the care team to uphold their commitments to deliver high-quality client care and to meet their obligations to their regulatory colleges.

There may be other risks specific to particular clients, which should be explored and discussed with clients directly.

Decisions to Implement a Restriction to Access Medical Records

After client makes a request for restriction to access their medical records and has spoken to a care team member about the impact that could have on their care, the Manager of Primary Care or Primary Care Provider will review, respond to, implement, and administer the requests (including on behalf of a Primary Care Provider, where applicable). Because the choice to implement a Restriction to Access Medical Records may have implications for the client's care, if applicable, the client's primary health care provider (e.g., Physician) must be involved in processing the request as appropriate.

The practical methods of implementing restrictions are varied; therefore, restricting access requests are considered on a case-by-case basis. A decision to implement a restriction will be based on the practicality of the solution, technological feasibility, and the specific circumstances.

The Manager of Primary Care or designate will notify in a timely manner any client, who made a Restriction to Access Medical Records request, of the decision made in respect of the restriction. If a decision has been to deny the request, the client will be informed of the right to make a complaint to the Information and Privacy Commissioner of Ontario.

Restriction to Access Medical Records Exclusions

Because of overall responsibility for care, a Restriction to Access Medical Records cannot be used to prevent the Primary Care Provider to whom the client is registered from accessing the client's record.

A Restriction to Access Medical Records is limited under PHIPA to those providing care to the client. It does not operate to prevent administrative functions from being carried out or the use or disclosure of PHI for other authorized purposes. For example, even where a Restriction to Access Medical Records is in place, it will not prevent a Primary Care Provider or Gateway CHC from engaging in legally permissible activities such as:

- Obtaining or processing payments
- Planning services
- Quality improvement
- Disposing of information
- Complying with a court order
- Litigation
- Research (with research ethics board approval)
- Teaching Staff to provide health care

The above actions are permitted under sections 37-50 of PHIPA.

A Restriction to Access Medical Records does not prevent Gateway CHC from using or disclosing PHI where there is a legal obligation to do so (for example, to fulfill mandatory reports to the Children's Aid Society or to the Ontario Ministry of Transportation). Gateway CHC may also use or disclose PHI if there are reasonable grounds to believe that using or disclosing the information is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. There may be other circumstances where the use or disclosure of PHI is required or permitted by law. The Staff Member should consult with the Privacy Officer when in doubt.

Therefore, it is important for any client requesting Restriction to Access their Medical Records to understand that some Gateway CHC administrative staff, including but not limited to the Privacy Officer, have access to records to

maintain all legal requirements as the Health Information Custodian (HIC), at all times.

Identifying a Client Chart Where Access Has Been Restricted

Before reviewing a client's PHI, Staff must always check to see if a Restriction to Access Medical Records has been applied. This will appear as a global alert on a client's chart.

- In the EMR, you will not be able to view anything but the demographics, the appointment history and the ability to book an appointment for a client for whom a Restriction to Access Medical Records has been implemented and from which you are excluded.

Staff should be aware of how records are made with restricted access and what such a restriction looks like. If you have questions, ask the Privacy Officer.

Electronic Records

If a client has implemented a Restriction to Access Medical Records on their chart, the chart is made private by the Manager of Primary Care or Primary Care Provider. When a user attempts to open the chart through the electronic medical record (EMR), the chart shows "PRIVATE".

If the Staff Member is restricted to opening the chart, then the electronic system will restrict access to that client's records by masking everything but the demographic sections. The rest of the chart will not be accessible to that user. The Manager of Primary Care can approve and implement a restriction or change the privacy settings on a client's chart when requested. The demographics section of the chart may be visible even if the whole chart is restricted, which includes:

- Client name, address, date of birth, all other demographics on the Patients window
- Physician, last billed date (if applicable), registration status, and all appointment history
- Ability to book appointments

This is still PHI and must be respected.

If a restriction pertains to specific Staff, their access will be restricted to the rest of the client's record or to a specific note.

If individual notes are restricted

Where individual notes in the chart are marked Private, the note field will be marked "*Private*".

Paper Records

Not Applicable; Gateway CHC does not have paper records.

"Breaking" the Restriction

If a Staff Member is authorized to access information that is otherwise "restricted", the following instructions explain how to access the PHI.

Electronic Record

The only people who can authorize a break in restriction are the Privacy Officer or Manager of Primary Care or designate. For emergency access to the chart, the user/provider must provide a reason for the access. With the Privacy Officer's consent, the Manager of Primary Care will lift the restriction of the chart for the user/provider to access for a set period of time. A lifting the restriction note (that cannot be deleted) is added to the client chart to indicate that the restriction was broken. Access to the health record is then available. After the set time, the user/provider will inform the Manager of Primary Care to re- apply restriction to the chart.

The other option to view a private record is to modify the client's privacy settings. Privacy settings, individual users and expiration dates on this access, can only be modified by the Manager of Primary Care or designate with the Privacy Officer's consent (for example, if reception needs access to scan the chart then access can be granted to one receptionist and that access can be set to expire at the end of the day).

Paper Records

Not applicable; Gateway CHC does not have paper records.

Any Staff Member who accesses PHI that is protected by a restriction must document on the client's health record the reason and authorization for "breaking" the restriction. All information subject to a restriction will be monitored and there will be random audits of such files. If Staff are in doubt about whether they are legally permitted to break a restriction, they should contact the Privacy Officer.

Of course, a client may choose to withdraw a restriction to access medical records request. That decision must be in writing

and documented on the health record, the same process for requesting a restriction.

Notice to External Health Care Providers

If a client's Restriction to Access Medical Records instructions state that the client does not want all or some PHI shared with an external health care provider, Gateway CHC will not disclose PHI to the restricted external health care provider unless:

- Gateway CHC is permitted or required by law to do so (for example, Gateway CHC needs to disclose the PHI to the external health care provider in order to reduce or eliminate a significant risk of serious bodily harm to the client or to another person or persons)
- The external health care provider has provided us with written proof of the client's express consent to the disclosure.

If Gateway CHC is prevented from disclosing PHI relevant to the provision of care to an external health care provider because of a restriction, Gateway CHC has an obligation to notify the receiving health care provider that not all the relevant PHI has been provided. As a note, the receiving health care provider is then able to explore the matter of the "restricted" information with the client and seek consent to have the restricted information shared.

Auditing and Review of Restricted Records

The Manager of Primary Care will maintain a confidential list of restricted charts and confirm that each restriction is configured as directed when it is implemented or changed.

The Privacy Officer or designate will review access to a restricted chart when requested by a client, when inappropriate access is suspected, or when the chart is selected for Gateway CHC's semi-annual random or high-risk EMR audit. The review will examine available access and override logs, confirm whether any temporary access permission has ended and the original restriction remains in place, and document the findings and follow-up.

Suspected inappropriate access will be referred to the Privacy Officer and addressed under the Privacy Breach Protocol. A client-directed restriction will not be removed solely because an audit is complete; changes to the restriction must follow the client's documented direction or another applicable legal authority.

Breach of Privacy

Unauthorized access by a Staff Member to a client's health record constitutes a breach of privacy and may result in disciplinary action up to and including termination of employment or contract.

The Primary Care Provider is obliged to notify any affected client(s) of a privacy breach and their rights and will do so in accordance with the requirements of PHIPA.

Attachments

Appendix B – Restricting Access to Medical Records Information Brochure

APPENDIX B – RESTRICTING ACCESS TO MEDICAL RECORDS INFORMATION BROCHURE

Restricting Access to Medical Records Information Brochure: How to Restrict Access to Your Health Record

You have a right to make choices and control how your health information held by Gateway CHC is collected, used, and shared, **subject to a few exceptions**.

You have the right to ask that Gateway CHC not share some or all of your health record with one or more of our staff members involved in your care, or ask us not to share your health record with your external health care providers (such as a hospital or specialist). This is known as asking for a "Restriction".

What is in your health record?

Your health record includes information such as your health history, care Gateway CHC has provided, family history, your medications and results from lab tests and notes from your health care providers within Gateway CHC or your other health care providers. If you would like a copy of your health record, please contact Gateway CHC medical record department to obtain the form.

Who sees your health record?

Only Staff who provide health care and services to you and Staff who do administrative tasks to support health care are authorized to look at your health information, and only when they need to see that information to do their job.

Gateway CHC uses your health information to make sure we can give you the best care. Your health information is shared only within your "circle of care" - meaning the Physicians, Nurse Practitioners, Nurses, Mental Health Counsellors, Social Workers, Client Resource Workers, Client Outreach Workers, Community Health Workers, Dieticians, hospitals, specialists, community services providers and other people and organizations that help with your care - unless Gateway CHC is permitted or required by law. Gateway CHC will not share your health information with anyone else - for example, your family or friends, employer, school or insurance company - unless we get your permission (known as "express consent") to do so or unless we are permitted or required by law (see "Restricted Access Exceptions" below).

What is "Restriction to Access Medical Records"?

Generally speaking, a Restriction to Access Medical Records means that all or part of your health information will be separated from our usual filing systems. If it is an electronic record, it will have additional restrictions of access. While all our health records are safely and securely stored, it restricts the access to your health information from certain people or institutions.

Are there risks to having a Restriction to Access Medical Records?

There are some risks when restricting access to your health information that you should consider before making your decision:

- Your health care providers may not have the information they need to give you the best possible care in a timely manner.
- Your health care providers may not have enough information to safely provide you with services and so may not be able to offer you care.
- It may be harder for your health care providers to share your information in an emergency.
- There may be errors in assessments, treatment or medications if the people providing care do not have enough information or do not have the right information about you.
- You may have to undergo duplicate tests, procedures and health history questions if existing information is unavailable.
- You may not benefit from the wide range of services Gateway CHC can offer you.
- There may be other risks specific to you and your request, which Gateway CHC will discuss with you. You can ask us questions about the specific risks that could come up depending on your choices.

Restriction to Access Medical Records Exceptions

Under the law, there are times when Gateway CHC is allowed to or must collect, use, or share personal information about you without your permission - even if your information is otherwise "restricted".

If your information is already restricted, the "restriction" may be broken and your information may be used or disclosed as permitted or required by law. Gateway CHC has provided some examples, but there may be other situations where the use or disclosure of your information is permitted or required by law. Gateway CHC may use or share your health information

without your permission in order to, for example:

- Report a child in need of protection to the Children's Aid Society
- Make reports to the Ministry of Transportation or Public Health or other mandatory reports
- Protect you or someone else if Gateway CHC believes there is a significant risk of serious harm
- Obtain or process payments
- Plan our services
- Engage in quality improvement exercises
- Dispose of information
- Comply with a court order
- Defend ourselves in litigation
- Engage in research (as long as Gateway CHC has research ethics board approval)
- Teach our staff to provide health care

If you have questions about how Gateway CHC can use or share your health information, you can ask a team member or the Privacy Officer**.**

How do you request a Restriction to Access Medical Records?

You can discuss any concerns regarding the privacy and confidentiality of your health information and your Restriction to Access Medical Records options with your Physician or health care provider. In some cases, you may not need a restriction in order to protect your information and Gateway CHC can discuss alternatives or options with you. For instance, you do not need a restriction to prevent health care professionals who are not involved in your care from viewing your personal information as these professionals are not within your "circle of care" and are therefore already not permitted to access your information on the basis of our policies and privacy laws.

You can submit your Restriction to Access Medical Records request in writing using our Request Form for Restricting Access to Medical Records, which you can get from our front desk. The completed form will be sent to the Program Manager.

Restriction to Access Medical Records requests are processed on a case-by-case basis. The Program Manager or designate will review and respond to the requests and will speak with your Physician or health care provider. Gateway CHC may not be able to accommodate every request - but Gateway CHC will explain any limits with you. Gateway CHC will tell you when the restriction is in place. You can also request that the restriction be removed at any time by contacting the Program Manager, Physician, or designate.

Information and Privacy Commissioner/Ontario:[7]

2 Bloor Street East, Suite 1400 Toronto, Ontario M4W 1A8 Canada

Telephone

Toronto Area: 416-326-3333

Long Distance: 1-800-387-0073 (within Ontario)

Fax

416-325-9195

[7] The office responsible for reviewing the privacy-related decisions and practices of health care institutions, such doctor's offices and family health teams, investigating privacy complaints made under the access, privacy and personal health information laws, and educating the public about such laws and access and privacy issues.

SAFEGUARDS FOR CLIENT INFORMATION GUIDELINES

CONTEXT AND PURPOSE

These guidelines are part of the *Privacy Policy*.

Gateway CHC holds a lot of personal information about our clients[8]. This information is sensitive and valuable to our clients, and Gateway CHC is obliged by law to treat it carefully. As part of our duties Gateway CHC must take all steps to keep client information safe and make sure that it can be accessed only by those who need to see it for a proper reason.

This applies equally to our electronic medical record, paper copies of health records, reports, test results, voice messages, emails and any other ways client information can be recorded. Gateway CHC must protect this information from loss, theft, unauthorized access including any kind of disclosure to the wrong people.

Following these guidelines will minimize the risk of client information falling into the wrong hands which could cause harm and distress to clients and legal consequences to Gateway CHC. Gateway CHC require everyone who is affiliated with Gateway CHC, including all staff, providers, volunteers, (including Board Members), students and vendors (collectively "Staff") to follow the best practices described here. Every Team Member has a role in keeping our clients' information secure, and Gateway CHC expects everyone to fulfill that role.

GUIDELINES

Restricted Access to Client Information

Access to client information is provided on a need-to-know basis as appropriate to the Staff's role and purpose for access. Staff will have access to only the minimum amount of personal health information necessary to perform their duties.

No snooping!

Staff must not access any health records unless authorized - which means only for legitimate reasons. **Staff may not access health records of their spouses, children, parents, friends or neighbours, or work colleagues unless that person is under the Staff's direct care or the Staff Member is authorized as part of their official duties (or if covering the shift or tasks for someone who is authorized).** Staff may only access their own health record (if applicable) through the normal client access channels and not directly using their EMR sign in as a Staff Member.
Staff must not:

- Access client information for "self-education" or out of curiosity or personal interest
- Edit, cut-and-paste, delete from or otherwise change any health records except for legitimate reasons Staff should know that all access to the electronic medical record is logged and audited.

Accounts and Passwords

Our information technology systems are protected by the use of personal accounts and passwords. Individual accounts are given access to information required by the account holder.

Gateway CHC requires all Staff to:

- Use only their own user account and password. Not permit anyone else to use their account
- Help maintain security by choosing hard-to-guess passwords
- Contact the Privacy Officer if they suspect any kind of computer misuse

A good privacy password is a mix of numbers, upper and lower case letters and symbols. Avoid using your name in a password.

An unauthorized person trying to gain access to our health records may not be obvious. Data breaches have occurred in other organizations after "confidence tricks" convinced individuals to reveal passwords or other information to intruders, for example, claiming to be the "IT helpdesk". Never tell anyone your password no matter who they say they are. If anyone you do not know requests information from you, you must verify their identity and their reason for asking first. If you are left in any doubt contact the Privacy Officer immediately.

[8] Gateway CHC has used the term "client" throughout the policy. It is possible that Gateway CHC holds PHI about individuals who are not clients, and the safeguards policy would apply equally to those individuals

Physical Security On-Site

Gateway CHC holds a large amount of client information in printed format - on paper, in files, and binders. Day timers, schedules, and notebooks may also contain client information and are confidential just like client files.

Access to client information is permitted by individuals who require the information to do their authorized jobs. If clients or visitors are in areas where client information is kept or in other private areas, politely challenge them as to their business. If there is any doubt as to someone's purpose, they should be asked to leave.

Client information in paper format should be kept in a locked cabinet, container or room. If a filing cabinet or room where client information is stored is not in constant use, it should be locked.

Where records are on desks in occupied rooms or in boxes they should be turned over so they cannot be read by someone nearby.

Client identifiable labels on files should not be visible to visitors.

Client information that is being stored before secure destruction will be kept separate and clearly marked.

Client Information in Transit

Because of the serious risk of loss or theft, client information will only ever be removed from the premises by those Staff who have a real need to do so to carry out their duties (for example, Staff who provide care to clients off-site such as home visits or community settings). This applies to electronic files, paper copies and information on laptops, smart phones, disks, and memory sticks (USB keys) and any other formats.

For electronic files, remote access to client information should be through our secure server, where Gateway CHC can protect it. Every time client information is saved to a laptop, disk, or memory stick there is a chance it may be lost or stolen. Therefore, Gateway CHC will do this only when absolutely necessary to carry out our jobs.

Where there is no choice but to take information off-site, client information will be de-identified if possible. Otherwise, if Staff are ever required to copy client information onto a laptop, memory stick or other portable device strong encryption must be used. Strong encryption is more than just password protected. If you are not sure how to do this, please contact the IT department. For paper files, keep papers in a locked box or bag for transport.

When in public, steps should be taken to avoid drawing attention to the materials (such as keeping them in an unmarked bag or container).

Laptop computers, disks or files containing personal health information must not be left on the seat or in the trunk of an unattended car, even for just a few moments.

When transporting client information, go directly to the destination, making the journey as short as practicable.

Client information should not be stored at home except in very limited circumstances and if the Team Member is required to keep information at home, it must be held securely and care should be taken to avoid family or friends or other visitors from having any access. Staff should not make printouts from remote access at home.

Sending Client Information

Special care must be taken when sending correspondence about a client or containing client information to anyone outside of Gateway CHC - including to another health care provider, to a third party, or to the client.

In addition to this policy, physicians and interdisciplinary health providers (collectively, “clinicians”) need to follow their own regulatory College’s directives on confidentiality, security of personal health information and communicating with clients to ensure privacy is protected.

External Emails and Text Messages

Because of the insecure nature of emails, Staff are not permitted to include client information in any email or text sent to a recipient other than to a Gateway CHC email address or Staff’s phone, except as set out below.

Clients

Clinicians may send or give permission to a Staff Member to send emails to their clients for the purposes of:

- Reminding clients about appointments and follow-up visits;
- Sending information or resources requested by a client;
- For requesting feedback to programs, groups or services that a client may have participated in;
- Assisting a client with self-management;
- Diagnostic imaging or other testing requisitions.

Any other information communicated with a client via email will be done on a limited basis and through an approved, secure and encrypted method, such as OCEAN. No emails to clients should be sent through unapproved programs such as “Gmail”. This is important because it:

- Decreases the chances of typos in entering email addresses
- Ensures that a copy of the email is recorded in the client’s chart under ‘email-email communication between client-provider’ notes for continuity of care and legal purposes
- Ensures that the email is sent from an approved email address so that automatic reply functionality is working properly
- Ensures that any information not intended for the client is not accidentally sent (such as can be the case with the “reply all” functionality of regular email chains).

Except in rare circumstances (such as an emergency where there is no other reasonable option), email (especially unencrypted email) should not be used to communicate diagnoses, provide information about test results or transmit other personal health information that will require a follow up. Clinicians must take care to consider the sensitivity of the information being conveyed over email (especially unencrypted email). Clinicians should also consider that as the volume and frequency of emails increase – so too does the risk inherent in communicating by email.

Gateway CHC only communicates by email from professional email accounts. Gateway CHC does not use personal email accounts to communicate with clients.

Gateway CHC recommends to clients that they use a password -protected email address that only they can access.

- The client must sign a Client Consent and Release for Ocean
- Email Communication and it must be documented in the client’s health record;
- Before sending, the Staff Member must check the email address carefully to confirm it is going to the correct recipient (NOTE: email programs that “autofill” the recipient field can insert an address you did not intend to send to); the following steps can help avoid misdirection:
    - Verify the recipient’s identity by sending a test message in advance and asking for confirmation to ensure the message reaches the intended recipient;
    - Confirm email addresses are up to date;
    - Ensure that the recipient’s email address corresponds to the intended address;
    - Regularly check pre-programmed email addresses to ensure that they are still correct.
- The Staff Member should not use the “reply-all” feature if responding to an email from a client and limit the number of recipients to the minimum necessary;
- To avoid mistakes, the Staff Member must check to see if there are any unexpected attachments to the email that will be sent (by clicking on “preview” to see the email content or otherwise reviewing the email before sending);
- If appropriate, the email message must be copied and entered into the health record or the clinician must write a note in the health record summarizing the clinically relevant information from the email communication; and
- The email may only include the minimum amount of personal health information necessary for the purpose.

For group emails (that is, emails to more than one client such as for flu clinics or client satisfaction surveys), only the Ocean secure email portal should be used. If Ocean is not feasible due to clients being associated with community programming and not registered to Gateway CHC’s Primary Care Team, check to make sure content is correct before sending including for any attachments that have been accidentally included. Keep in mind large emails have an increased risk of privacy breaches and extra care must be taken.

As part of protecting information communicated by email, Gateway CHC also:

- Acknowledge receipt of emails;
- Inform clients of any email address changes; and
- Store personal health information on email servers only for as long as is necessary to serve the intended purpose. For example, if email communication is documented in the client’s record, it may not be necessary to retain duplicate copies of the information on an email server. Likewise, Gateway CHC ensures that all copies of emails containing personal health information on portable devices are securely deleted when they are no longer needed and are documented in the client’s record.

The Privacy Officer ensures that Gateway CHC as an organization:

- Restrict access to the email system and to email content on a need-to-know basis; Ensure strong access controls to email accounts used by clinicians; and
- Remind employees, other agents, and clients of the risks associated with phishing to avoid falling prey to malware, spyware, or other forms of social engineering.

Similar issues arise with use of text messages. Text messages should be used for reminding clients about their

appointments and follow-up visits only.

Emails Sent within Gateway CHC

It is preferable to send messages about clients through the electronic medical record functionality wherever possible.

If sending emails within the Gateway CHC, limit the personal information included to the minimum necessary. Refer to clients by their initials rather than using their full names, if it is possible to do so.

When using the “reply-to” feature there is a risk of including more information than necessary by including a copy of the original email. Therefore, start a new email rather than responding to an email thread.

Carefully check the recipient before hitting the send button. Email programs that autofill the recipient field can insert an address you did not intend to send to.

Do Not use the "reply-all" feature and limit the number of recipients to the minimum necessary.

- Please note that ANY emails sent about a client, either via Ontario Health approved email service vendor to external providers, and/or within Gateway CHC, are considered PHI and should be documented in the EMR. Ideally the email should be copied and pasted to the EMR under the heading: email – Email communication.

Accessing Email on a Mobile Device

If a Gateway CHC email address is to be accessible on a mobile device (such as a smart phone) any loss of the device must be reported immediately to Gateway CHC IT, so their email address is inactivated temporarily.

Facsimile (Faxes)

Misdirected faxes are easy to send and difficult to correct. They make up a significant proportion of privacy breaches. “Quick codes” are stored in the fax machine for numbers used more than once and should be used if available. Otherwise, when sending client information by fax, carefully check the fax number - multiple times - to ensure it is correct.

Include a cover sheet stating for whom the fax is intended. The cover sheet must ask a recipient to call if information is received in error.

Where appropriate, call the recipient prior to sending a fax so they can be waiting to retrieve it.

After sending a fax, collect and keep a confirmation receipt. If there is any question about a wrong number being used the receipt will make it much easier to check and to retrieve information sent to the wrong place.

A privacy breach occurs whenever client information is sent to a third party without the client’s authorization or without being otherwise permitted or required by law. There can be particularly significant consequences in cases where clinicians repeatedly send client information to a third party improperly.

In the event of a misdirected fax containing client information, it is important to ask the wrong or unintended recipient to confirm **in writing** that the information was destroyed and not kept or shared with anyone. This should then be documented in the client’s chart.

Clinicians should use their judgment when it comes to implementing the *Privacy Breach Protocol* as a result of a misdirected fax. For single instances of a fax that is misdirected to another health care provider, ensuring that the recipient securely destroyed the fax may be sufficient. Clinicians may choose to put a reminder in the chart to discuss the breach (and actions taken to correct it) next time the client visit the clinic. Clinicians should be aware that they may face increased consequences if they do not implement the full *Privacy Breach Protocol* whenever a breach occurs.

Please report all stray faxes to your Privacy Officer. And situations where there are repeated stray faxes must be reported to the Privacy Officer to assess whether a report to the Information and Privacy Commissioner is required and how to notify affected individuals.

If you receive a stray fax (meaning you receive a fax that was not intended for anyone at our organization), please notify the sender of their error as soon as you discover it. If you notice a pattern of such stray faxes received from the same sender in error, please notify the Privacy Officer.

Social Media

Staff are advised to avoid posting information about client-specific cases or and are advised against providing medical or other clinical **advice** online. Regulatory colleges and professional liability indemnity providers recommend that clinicians avoid posting comments in internet discussion forums or other online groups to avoid the perception of providing medical or health care **advice**. While it may be acceptable to provide general health-related **information** for public or professional educational purposes, those purposes should be clearly identified and clearly marked as not providing advice.

Telephone

Clients may ask us to relay their own health information to them by telephone. Calling a client at home or at work or leaving messages is an everyday reality that carries a real risk to our clients' privacy. It may be difficult to verify the identity of the person who answers or control who hears a message.

To minimize these risks, ask clients every time they register for an appointment to check that their contact information is up to date so Gateway CHC has their most recent telephone numbers (and home address – see **Mail** below). Ask if Gateway CHC can leave a message with someone or on an answering service and confirm the number.

If Gateway CHC has the client's consent to leave a message and you are answered by a machine, listen for clues that you may have misdialed before leaving a message. For example, if the message repeats a name or number other than the one you expected to hear. If you are in any doubt leave a message only to say to call the office.

If a client calls Gateway CHC must take steps to confirm the caller's identity before providing information. Our clients expect it. If Gateway CHC are in doubt as to the identity of the caller, we can confirm the caller's identify by asking questions such as:

- What is your date of birth?
- What is your health card number?

If speaking on the phone with a client in a place other than the office, Staff should ensure that no one can overhear the conversation (for example, if at home, no family members of the Team Member, or if anywhere else such as outside or in a coffee shop, no passerby or others nearby).

Mail

Sometimes it is necessary to send client information by mail or courier. When sending information in the mail, check the address to make sure it is correct. Also, mark the envelope or package "Attention <name>" on the outside to make sure it is opened only by the intended recipient.

Make sure that no health information can be read through the envelope or window, and consider whether there are any logos or other markings on the envelope that may identify the nature of the content enclosed.

For highly sensitive information, obtain a tracking number and follow up with the client to make sure it was received. When sending regular client information via mail, a tracking number is not mandatory, but should be used depending on the sensitivity of the health information being sent. For less sensitive information, clinicians may choose to mark envelopes with a CONFIDENTIAL stamp and include a return mailing address.

The easiest way to prevent the chances that a client's mail will be lost or stolen (without using a tracking number system) is to call the client and ask them to pick up the letter at the office. If they are not able to attend, the client's home address can be confirmed at that time, and they will have notice that they will receive a letter in the next few days.

Virtual Care

Due to the lengthy protocols around Virtual Care/Working Remotely, there is a separate policy entitled: Virtual (Video) Care Policy. It is included in the Privacy of Client Information Policy and Procedures.

Filing Client Information

Care should always be taken when tagging and filing electronic records or uploading paper copies of client information to a client's electronic health record to ensure the information relates to the correct client. Check client names and dates of birth carefully.

When client information is filed in the wrong health record, it should be corrected immediately. It may be appropriate to choose *not* to enact the *Privacy Breach Protocol* when a test result is filed in the wrong chart, if a clinician feels confident that the misfiled information was not accessed by another healthcare provider to make healthcare decisions on behalf of the client, and that no other client would have had access to the information (for example, through a request for a copy of the chart). If it is possible that the information could have been used to make treatment decisions or could have been shared with an unauthorized third party, then the *Privacy Breach Protocol* should be enacted.

Destroying Client Information

When client information is no longer needed Gateway CHC must make sure it is destroyed securely. Different methods of destruction are appropriate depending on how the data is stored:

Material	Appropriate Method of Destruction
Paper (e.g., printouts, faxes, letters, labels, etc.)	Shredding
Audio or video tapes	Shredding
Medication containers (bottles and bags) with ID labels	Shredding of label (or container) or return to supplier along with unused medications
Electronic devices with memory storage (e.g., laptops, PCs, printers, photocopiers, dictaphones)	Data wiping prior to redeployment or return to vendor – lease company
CDs, DVDs, disks, USB keys	Shredding or breaking into pieces
Pictures, slides	Shredding

Never recycle any paper or media which contains client information. Never treat any paper which has been printed with client information as reusable for scrap. When client information is no longer needed, it should be securely destroyed.

Please refer to the Records Retention and Destruction Policy for further information.

Third Party Vendors

When Gateway CHC hires outside contractors to do data entry or provide information systems or to store, transport or destroy client information, Gateway CHC only uses those that are bonded and insured and maintain a verifiable commitment to confidentiality. Gateway CHC makes sure that the contractor uses the methods documented in the contract we have with them.

Gateway CHC only selects contractors who commit under contract to:

- Agree to be a PHIPA agent of Gateway CHC
- Hold and follow written privacy policies and procedures saying how material is to be kept safe in transit, storage and destruction as applicable
- Have insurance coverage for their liabilities under contract
- Require their own personnel to sign confidentiality agreements
- Have appropriate training for their personnel on privacy policies and the procedures to implement them

Logging and Auditing in Electronic Medical Record Logging

Our electronic medical record logs user's access. The logs include for every instance in which a record or part of a record of personal health information is viewed, handled, modified or otherwise dealt with:

- The identity of the individual to whom the personal health information relates
- The type of information that was viewed, handled, modified or otherwise dealt with
- The identity of all persons who viewed, handled, modified or otherwise dealt with the personal health information.
- The date and time on which the information was viewed, handled, modified or otherwise dealt with.
- The fact of an override of a consent directive on the system (that is, if a lockbox has been overridden).

Audits

Access audits can be performed on any client record at the request of the Privacy Officer or at the request of a client.

Access Audit requests by client

Clients may request an access audit on their own medical record, or the record of a client for whom they are the substitute decision maker by:

- Submitting a written request to the Manager of Primary Care, Primary Care Provider, or designate and specifying that they would like a chart access report and the date range requested.

Random audits

Semi-annually, an audit of EMR activity will be performed on randomly selected client charts or charts identified by Gateway CHC as at high risk for unauthorized access. High risk clients may be clients who are famous, related to staff or for any other criteria chosen by Gateway CHC.

Audits of individuals on request

When an unauthorized access has been suspected or reported of an EMR user, an audit of their access will be performed.

Records of all audits will contain the following information:

- Demographic information (Client name, OHIP #) of client audited
- Reason for audit (e.g., request or random selection)
- Date range selected for audit
- Description of unauthorized or questionable activity and results of inquiry

Inquiry of unauthorized or questionable activity

Unauthorized or questionable activity will be brought to the attention of the Privacy Officer to determine the next course of action.

Unauthorized or questionable activity may be investigated in any of the following ways:

- Contact the user and ask for the reason for access
- Contact the client to inform them of the unauthorized access
- Perform an additional audit to determine if there has been any further unauthorized access

Breach of Privacy Safeguards

Failure by Staff to adhere to the privacy safeguards and guidelines set out above may result in corrective actions being taken. Such corrective action may include, but is not limited to, retraining, loss of access to systems, suspension, reporting conduct to the Information and Privacy Commissioner of Ontario or a professional regulatory body or sponsoring agency, school or institution, termination of contract, restriction or revocation of privileges, and immediate dismissal. Additional consequences include notification of affected persons, fines, prosecutions, or lawsuits.

APPENDIX C – TECHNOLOGY FACT SHEET – DISPOSING OF YOUR ELECTRONIC MEDIA

Technology Fact Sheet – Disposing Of Your Electronic Media



APRIL 2018

TECHNOLOGY
FACT SHEET

Smart Cities and Your Privacy Rights

New technologies promise to help municipalities better manage urban environments and deliver services in a more effective and efficient way. They can help to make communities more liveable, sustainable, and fair. Many involve the collection and use of large amounts of information, including personal information. Cities or municipalities that use these connected technologies are often described as "smart cities."

This fact sheet was developed to help members of the public understand smart cities and how they can impact an individual's privacy

The Office of the Information and Privacy Commissioner of Ontario (IPC) provides independent oversight of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). This act protects the privacy of personal information by setting rules for its collection, use and disclosure by municipalities and municipal institutions. These rules also give individuals the right to access their own personal information.

The IPC has developed this fact sheet to help the public understand smart cities and how they can impact an individual's privacy.

WHAT ARE "SMART" CITIES?

Smart cities use technologies that collect data to improve the management and delivery of municipal services, support planning and analysis, and promote innovation within the community. By collecting large amounts of data, often in real-time, municipalities can gain a greater understanding of the quality and effectiveness of their services. For example, commuter traffic flow data can identify congestion

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

hotspots and inform planning and urban design. Insights can also be generated by linking the collected data with other data sources and using analytics technology to uncover patterns and connections in large data sets.

This can lead to "smart" actions, such as:

- sending a signal to garbage collectors when sensors indicate that garbage bins are full
- turning on park water sprinklers when sensors detect the soil is dry
- synchronizing street lights with traffic flows
- directing self-driving vehicles to available parking spots using GPS information collected from the vehicles.

Information collected, used, retained and disclosed by smart cities can, and often does, include personal information

WHAT INFORMATION IS COLLECTED AND HOW?

Information collected, used, retained and disclosed by smart cities can, and often does, include personal information. For example, some smart city technologies collect information about individuals from their mobile devices, including information about their movements around the city.

Personal information can also be collected from municipally owned and operated sensors, such as audio and video recording devices, or vehicle licence plate readers.

Municipalities may enter into information-sharing agreements with third parties, such as smartphone app providers, or companies that install and manage sensors and communications infrastructure. These agreements may require or allow third parties to collect and use personal information for their own purposes as well as for the purposes of the municipality.

WHO OWNS THE INFORMATION?

Municipalities need to take steps to ensure that the non-personal information collected by their private sector partners is available as a public resource. They can do this by ensuring that their contractual arrangements do not give proprietary rights over the information to private sector partners who would use the data for commercial purposes.

A U.S. police service contracted with a software provider to compile and analyze information about criminal and civil matters. When the contractual relationship ended, the service lost access to a significant amount of data and insights generated during that time due to the software company's claims over intellectual property rights.

HOW CAN SMART CITIES AFFECT PRIVACY?

When municipalities use technologies to collect personal information for any purpose, they must comply with *MFIPPA*. Smart cities raise concerns about compliance with *MFIPPA* in a number of different ways. For example:

Unauthorized collection of personal information and surveillance

MFIPPA permits the collection of personal information by municipalities where it is necessary to administer their lawfully authorized activities. Any collection of personal information that exceeds what is necessary for those activities is not permitted.

Smart city technologies enable the collection of information about residents going about their daily lives—potentially creating personal profiles of individuals' behaviour, interests and interactions with others, especially when that information is combined with other information.

Great care must be taken to ensure that smart cities do not become infrastructures for mass surveillance

A major European city installed "smart" internet-connected garbage and recycling bins throughout the city featuring large video screens on each side to broadcast news, information and ads to the public. Unknown to passersby, the bins also collected signals from their Wi-Fi enabled devices, which can be used to identify individuals and track their travels. In the first month of operation, over a million unique devices were recorded. In response to a public outcry, the city shut down the "spying trash cans."

Personal information used for secondary purposes

MFIPPA limits how personal information can be used. The use limitations in the act are based on a key principle of privacy protection, which requires that, with some exceptions, personal information can only be used for the purposes for which it was collected, or for a consistent purpose. For example, personal information collected to assist with urban planning decisions should not be used to provide targeted advertising to individuals. Doing so constitutes an unauthorized secondary use under *MFIPPA*.

Smart city technologies such as gunshot detection systems use microphones installed on streetlights around a city to detect the location of gunshots and alert police quickly. These same microphones are also capable of recording street-level conversations for very different purposes.

Unauthorized disclosures of personal information

MFIPPA requires Ontario municipalities to have reasonable measures in place to protect personal information from unauthorized access and disclosure.

As with any complex, connected technology smart city systems are vulnerable to attacks by hackers. The more points of information collection, processing and access to the systems, the greater the risk of a security breach. Privacy breaches can also happen as a result of unauthorized access and misuse of personal information by individuals employed by the municipality or third parties.

Complex, connected technologies used by smart cities may be vulnerable to attacks by hackers

> A Canadian city that offered residents smartphone apps to track garbage, recycling and yard-waste pickup schedules discovered that the application's database had been hacked, exposing the personal information of thousands of residents.

There is a strong desire to make some information collected by smart city technologies publicly available to support innovation within communities. Municipalities need to take steps to ensure that any personal or identifying information has been removed from any data that is released to third parties, or made publicly available in support of open data initiatives.

HOW CAN PRIVACY RISKS BE MINIMIZED?

Good planning and design can minimize risk and ensure that individual privacy is protected. To protect privacy in smart city projects, municipalities should take a number of steps, including:

- Conducting **privacy impact and threat risk assessments**. These are widely recognized tools to identify privacy and security risks, and the measures needed to reduce those risks. They should be conducted when designing new technologies and programs involving the collection of personal information.
- Applying a **data minimization** approach to the design and operation of the technology. This means that municipalities should ensure they, and any contracted third parties, do not collect, use, retain or disclose personal information if other information will serve the required purpose. In all cases, where the goals can be achieved using less privacy invasive alternatives, those alternatives should be pursued.
- Ensuring that when it is necessary to collect personal information, steps are taken to remove any identifiable information at the earliest opportunity. Wherever possible, municipalities and their agents should only use, retain, and disclose **de-identified** information.

- Putting in place a privacy and access **governance** program that includes comprehensive security policies and procedures, strong oversight of third parties, and privacy breach response policies. The program will also need to include ways for individuals to exercise their right to access their own personal information.
- Ensuring **community engagement** and **project transparency** to help all members of the public understand how they might be affected and what options they may have to participate and provide input.
- Obtaining informed **consent,** where required by law**,** directly from the individuals whose personal information may be used and disclosed or requiring the third parties involved to get consent. When possible, individuals should be allowed to opt out of participating.

Good planning and design can minimize risk and ensure that individual privacy is protected

WHAT IS THE IPC DOING TO PROTECT MY PRIVACY?

The IPC is committed to ensuring your privacy is protected. Smart cities create new challenges and opportunities for Ontario's municipalities and communities. We believe that with careful planning and education about the unique issues raised by smart city technologies, personal information can be collected and used in a privacy-protective way. The IPC is working with local and national leaders to encourage transparency and ensure that privacy protections are built into smart city initiatives.

WHAT RIGHTS DO I HAVE UNDER ONTARIO'S PRIVACY LAWS?

It's your community too. You can help shape its future and protect your own personal information and privacy.

If you have questions about what personal information a municipality is collecting or how it is being used, consult their website or contact them for more information.

If you would like a copy of the information a municipality has about you, you can file an access to information request. To learn more about making an access to information request and what you can do to protect your privacy, visit the IPC's website: **www.ipc.on.ca**.

ADDITIONAL RESOURCES

- **What is Personal Information?**
- **Big Data and Your Privacy Rights**
- **Open Government and Protecting Privacy**

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Electronic communication between providers:

When healthcare providers use email communication to share patients' information, they must adhere to strict privacy and security standards to protect patients' confidential information and comply with regulations. Using email communication between healthcare providers for sharing patients' information. Emails should not contain any health information or clients' identifiers unless e-mails are encrypted.

Secure Email Communication

Encryption: All emails containing patients' information must be encrypted using a secure method to protect the confidentiality of the information during transmission.

Secure Email Accounts: Healthcare providers and staff must use the organization's secure, password-protected email accounts to send and receive emails containing patients' information.

Minimum Necessary: Healthcare providers and staff must include only the minimum necessary information in email communications to achieve the intended purpose.

Gateway Community Health Centre

VIRTUAL (VIDEO) CARE POLICY

PURPOSE

This policy and the consent form explain how Gateway CHC will maintain to offer virtual care.

POLICY STATEMENT

Due to the state of emergency declared in Ontario related to the COVID-19 pandemic, Gateway CHC introduced virtual visits in April 2020, to comply with social distancing requirements issued by local, provincial, and federal public health authorities. Gateway CHC continues to provide virtual health care although provincial government and public health regulations regarding COVID-19 protocols have been relaxed and/or eliminated.

PROCEDURE

Selecting the Most Appropriate Virtual Care Platforms

Virtual care may be provided by telephone, video visit, or secure messaging. To determine which type of virtual care is most appropriate, Gateway CHC staff, providers, and contractors, will consider client: reason(s) for accessing Gateway CHC programs/services, preferences, as well as barriers for reasons including language, impaired mobility/hearing/vision, and limited access to technology.

Approved Technology

The following virtual care technologies are approved for use at Gateway CHC:

- Ontario Telehealth Network (OTN)
- Zoom Professional (with or without webcam) for community support groups
- Office 365 Teams
- Ocean – a software added onto the EMR for Online Appointment Booking and Secure patients' messaging

Service providers who wish to use other technology for virtual care must seek and gain approval from the Privacy Officer before use.

Documentation - Recordings and Photographs

Neither service providers nor clients are permitted to video or audio record virtual visits. Exceptions may be made if clients request to record/video their visit due to disabilities and/or difficulties retaining information. Providers and clients should discuss this option before sessions so that all parties are aware of the intention to record/video the visit.

Photographs (for example, of skin conditions) are appropriate if it will improve client health outcomes. Service providers must ask clients for permission before taking photographs and saving it in the Electronic Medical Record (EMR).

Service providers must document all virtual visits in client charts as **in-person visits**.

Verbal consent for virtual care, recordings, and/or photographs must be documented in the EMR for each virtual video visit. EMR macros (templates) may be used.

Working from Home/Remotely

Working from home creates additional challenges for client privacy, clinical professionalism, and boundaries. Service providers and staff must adhere to best clinical standards and practices to safeguard personal health information (PHI).

Best Practices to Safeguard Personal Health Information (PHI)

1. **Devices:** Providers must access the EMR through FortiClient with MFA (Multifactor Authentication).
2. **Private Space:** A private room is necessary so that no one, with whom you are sharing space, can see or overhear virtual visits.
3. **Technology**:
    a. Use firewalls and protection against software threats.
    b. Update applications regularly with the latest security and anti-virus software

c. Use Mobile Device Management software for all Gateway CHC mobile devices.
d. Use encrypted USBs for transfer of PHI (ensure USBs are opened on IT approved standalone computer).
e. Use and maintain strong passwords.
f. Do not share passwords.
g. Do not post meeting ID, room ID, or other consultation identifiers publicly.
h. Do not use public Wi-Fi.
i. Do not click on any suspicious emails especially related to "invoices" or "change your password". These are likely hacking attempt emails.
j. Verify and authenticate a client's identity before engaging in video visits.
k. Confirm client email addresses before initiating email exchanges.
l. Lock the computer when it is not in use. Apply short cut *Alt+F12* to lock the EMR screen.

4. **Paper:**
   a. Keep papers in a locked box or bag for transport and do not leave files in your car or public transit.
   b. Do not leave paper that has personal health information on it available to anyone else while working from home.
   c. When not working, keep all paper for work in a bag, locked room, or some other secure place. Care should be taken to avoid family or friends or other visitors from having any access to your work.
   d. Paper records no longer needed must be shredded with a crosscut or other confetti shredder. Alternatively, paper records may be brought back to the workplace for secure destruction as early as possible. Do not put paper records containing personal information in the garbage or recycling.
   e. Note: Removing someone's name from a record does not necessarily anonymize the record and it is not an acceptable practice.
5. **Phone:**
   a. It is recommended that providers block personal phone numbers when using personal devices for virtual visits.
   b. Work phones should be forwarded to cellphones so that clients can still call providers directly using the Gateway CHC number and corresponding extension.
6. **Consultation and Debriefing:**
   a. Service providers need to let all Gateway CHC staff know that they are available to clients for remote consultations/visits or debrief related to healthcare service delivery.

If the service providers anticipate experiencing difficulties following the Best Practices to Safeguard PHI, they must have a discussion with their direct supervisor to explore whether other options to establish appropriate work arrangements can be made. These options should be approved by the Privacy Officer (or Delegate) to ensure appropriate protection of PHI.

Privacy Protection

Cyber-attacks are a growing concern during the pandemic. Staff need to be vigilant in protecting client privacy and confidentiality. Staff need to inform the Privacy Officer immediately if they suspect their records or a virtual visit has been comprised.

Administrative Safeguards

Cyber security threats are monitored and addressed by:

- Updating software regularly.
- Ongoing email reminders to staff to support the detection of phishing attempts.
- Conducting regular threat risk assessments.

Notice to Participating Clients

Staff should reference the Consent Form for Audio and Video Technology for Virtual (video visit) Care to explain to clients what a virtual visit entails and ask for their written consent to the terms. Staff must also provide clients a copy of the consent form or email them a written copy through the secure Ocean email portal.

Prior to booking a virtual visit with clients, staff should explain that virtual visits and should share the following information with clients:

1. **Description:**
   - Gateway CHC uses video and audio technology, so service providers and clients can see and hear each

other.

- Gateway CHC asks staff be in quiet, private places for virtual visits, so that others cannot overhear the sessions. Gateway CHC recommends that clients use a quiet and private place for virtual visits, so that others cannot overhear the sessions. If, on occasion, the client wants to include others in the virtual session, they must inform the care provider in advance.
- A client will be asked details of their health concern and their health history. These questions may be very personal and sensitive.
- Details of the virtual visit will be documented in the client's health record like an in-person visit.
- Gateway CHC will not record/video the virtual visit. Gateway CHC asks clients not to record the visit either. Exceptions may be made for clients who have disabilities/difficulties retaining information. In these exceptions, providers should be notified of clients' intention to record/video the visit before the session begins.
- As part of the course of treatment, the care provider may need to take a photograph during the session; however, the provider will obtain the client's permission before any photograph is taken.

2. **Limitations:**

- Virtual visits are not appropriate for emergencies. If a client is experiencing an emergency, they need to call 9-1-1 or proceed to the Emergency Department.
- Virtual visits are not appropriate when a physical examination is required.
- Virtual visits may not always be applicable, but can be determined on a case-by-case basis

3. **Privacy:**

- Gateway CHC has taken appropriate steps to preserve client privacy based on this emergency situation.
- Gateway CHC service providers who are conducting virtual visits may be working from home or remotely. For this reason, Gateway CHC cannot provide a client with the same guarantee of security and confidentiality as if they were seen in- person and on-site. Staff are asked to conduct virtual visits in private, away from others.

4. **Feedback (After the Completion of Virtual Care Visits):**

   Service providers should provide an opportunity from clients for feedback to ensure they feel secure using digital platforms and that they are not reluctant to share information for fear of privacy and security risks.

Privacy Breaches

All privacy complaints, incidents, and actual or potential breaches must be reported immediately to the Privacy Officer, so that they can implement the Gateway CHC Privacy Breach Protocol. Examples of breaches in the virtual care context include:

Video:

- Video launches from a public space.
- Wrong client being invited to participate in a video virtual visit.
- Wrong client attending a video virtual visit.
- Wrong clinical user invited to or attending a multipoint video virtual visit.
- Video virtual visit launched in error after a client's virtual visit is cancelled.
- Sharing information for the wrong client during a video virtual visit.

Secure Messaging:

- Messages containing PHI sent to a wrong client.
- Attaching PHI for the wrong client to a message.

Risks Associated with Virtual Visits:

- It is possible that there could be a problem with the technology and the client's virtual visit could be cut short or interrupted.
- The quality of the video or audio may not be good enough for a healthcare provider to assist virtually and could negatively impact the quality of care received.

OPTIONS AVAILABLE:	Not Applicable
ADMINISTRATION:	Privacy Office
RELATED REFERENCES:	Privacy Policy Privacy Breach Protocol Remote Work Policy Emergency Preparedness Plan (Pandemic Plan)
FORMS/PAPERWORK:	Virtual Care Client Consent Form

Gateway
Community Health Centre

PRIVACY BREACH PROTOCOL

PURPOSE AND CONTEXT

This is part of the *Privacy Policy*.

Report

All privacy breaches must be reported immediately to the Privacy Officer.

Privacy Breach

A privacy breach happens whenever a person contravenes or is about to contravene a rule under the *Personal Health Information Protection Act, 2004* (PHIPA) or our privacy policies. The most obvious privacy breaches happen when client information is lost, stolen or accessed by or sent to someone without authorization.

For example:

- Our sever is hacked and held ransom after an email with a virus is opened
- An unencrypted laptop with health information saved on the hard drive is stolen
- A courier package of client records is not delivered to the correct address
- An unencrypted USB key with an Excel spreadsheet with client information or Word files is lost
- A client reads another client's health record on a computer while waiting in a clinic room
- A Staff Member talks about a client with a personal friend
- A Staff Member takes a picture or makes an audio or video recording of a client without consent of the client
- Staff Member sends an email to a "help desk" attaching a worksheet with client information but does not check the email address and instead of sending the attachment internally – sends it to the last help desk emailed which is at a bank
- Health records to be disposed of are recycled and not shredded
- Out of curiosity, a Staff Member reviews a neighbour's health record
- A student or any other Staff Member looks at health records of clients on a self-initiated education project without being assigned to those clients and without specific authorization for an approved educational exercise
- A fax with client information is misdirected to a business where the fax number was entered incorrectly
- Health information is given to the media
- A Staff Member makes a copy of an ex-spouse's health record without it being part of the Staff's position to do so
- Staff discuss clients in hallways and lunchrooms and other clients overhear (even colleagues overhear)
- A Staff Member releases information to another health care provider when a client has said they do not want that provider to know
- A Staff Member releases information to a spouse when the client doesn't want that spouse to know
- A Staff Member releases information to a child's parent when the child is capable of making their own decisions and said don't tell their parents
- Scheduling or appointment confirmation or reminder notification for a virtual visit includes an excessive amount of personal health information.
- Virtual video visit launches from a public space
- Wrong client is invited to participate in or attends a video virtual visit.
- Wrong clinical user invited to or attends a multipoint video virtual visit
- Video virtual visit launched in error after a client visit is cancelled
- Sharing information (e.g., test results) for the wrong client during a video visit
- Clinical users or staff given unauthorized access during an encounter or to the videoconferencing system.
- A video virtual visit is recorded without authorization.
- Messages containing PHI sent to the wrong client via email
- Unauthorized clinical users reviewing client requests and messages without their consent.
- Unauthorized clinical users copied on a message sent to a client.

PROTOCOL

The following steps will be taken by the Privacy Officer (or delegate) if they believe there has been a privacy breach:

Step 1: Respond immediately by implementing the privacy breach protocol

- Ensure appropriate individuals are immediately notified of the breach, including the Privacy Officer and the physicians or other health care providers whose clients are potentially affected by the privacy breach.
- Address the priorities of containment and notification as set out in the following steps.
- Consider engaging legal counsel or a privacy breach coach if appropriate.
- Consider notifying the Information and Privacy Commissioner/Ontario (IPC/O) (www.ipc.on.ca). As time passes, the Privacy Officer will revisit this need to report on an ongoing basis. It may be premature to report if unclear whether there has been a breach or if unclear of the scope of the breach. The Privacy Officer may need to keep the IPC/O apprised through this process.
- Consider when to notify the insurer (which may be a condition of coverage), the Board Chair, and other key internal stakeholders.
- Finally, fill out an incident report

Step 2: Containment - Identify the scope of the potential breach and take steps to contain it

- Retrieve and secure any personal information that has been disclosed or inappropriately used or collected (including all electronic or hard copies). This might include attending the scene to determine whether there are any other records in public.
- Ensure that no copies of personal health information have been made or retained by the individual who was not authorized to collect, use or receive the information. Obtain the person's contact information if follow-up is required.
- Determine whether the privacy breach would allow unauthorized access to any other personal health information (e.g., an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords or identification numbers, temporarily shut down a system, suspend an individual or group's access to the system, implement security, institute a restriction to the file).
- Consider notifying or updating the IPC/O and/or legal counsel if appropriate.

Step 3: Clarify the facts

- Consider whether there is sufficient expertise to conduct an internal investigation or whether a specialist (such as a privacy or IT security specialist) is required
- Determine the scope of the breach:
    - Details of the incident and how it was discovered
    - Number of people affected
    - Who was involved
    - Dates
    - Type of incident, such as:
        - Unauthorized use
        - Unauthorized disclosure
        - Hacking, malware, security breach
        - Lost/stolen mobile device
        - Lost/stolen hard copies
        - Refused access or correction request
        - Fax to wrong number
        - Email to wrong recipient
- Determine how it happened and who was involved and why

Step 4: Notification - Identify those individuals whose privacy was breached and notify them of the breach

- At the first reasonable opportunity, any affected clients (or others whose personal health information has been affected) will be notified. Gateway CHC gives careful consideration to whether affected individuals need to know immediately (especially where despite our efforts, the breach is ongoing or where the information in question is of a highly sensitive nature or there is reason to believe that it will be used in a malicious way).
- The type of notification will be determined based on the circumstances (such as the sensitivity of the personal health information, the number of people affected, and the potential effect the notification will have on the client(s)).
    - For example, notification may be in person or by telephone or in writing, or depending on the circumstances, a notation made in the client's file to be discussed at their next appointment.
    - In some cases, a public notice is the most efficient and effective method of notice.

    - Gateway CHC focuses on considerations such as:
        - The potential privacy impact of calling the individual's home or sending a letter
        - Whether the affected individual will be coming in to see a health care provider very soon and could be told in person
        - Whether anyone affected is in a vulnerable state of health or deceased or a child or incapable to make informed decisions such that notice would be given to a substitute decision-maker and consider the best way to manage those sensitive issues
- Provide details of the extent of the breach and the specifics of the personal health information at issue
- Advise affected individuals of the steps that have been or will be taken to address the breach, both immediate and long-term.
- Establish a plan to address what clinical and administrative staff and others should do if they receive calls about the privacy breach
- Consider notifying the IPC/O and/or legal counsel if appropriate – especially if required by law

Step 5: Investigation and Remediation

- Conduct an internal investigation into the matter. The objectives of the investigation will be to:
    - Ensure the immediate requirements of containment and notification have been addressed
    - Review the circumstances surrounding the breach
    - Review the adequacy of existing policies and procedures in protecting personal health information
    - Address the situation on a systemic basis
    - Identify opportunities to prevent a similar breach from happening in the future
- Change practices as necessary
- Ensure staff are appropriately re-educated and re-trained with respect to compliance with the privacy protection provisions of PHIPA and the circumstances of the breach and the recommendations of how to avoid it in the future
- Continue notification obligations to affected individuals as appropriate
- Consider notifying the IPC/O and/or legal counsel as appropriate
- Consider whether it is necessary to call the police
- Consider any disciplinary consequences with staff or contract issues with independent contractors or vendors that follow from the privacy breach and any related obligations to report to regulatory colleges
- Close out incident report indicating the steps taken to address breach

Step 6: Recordkeeping

- Keep a record of all privacy complaints, incidents and breaches including investigations, notifications and remedial action taken.
- Statistics about breaches involving a theft, loss, or unauthorized use or disclosure of personal information must be submitted to the IPC/O annually, due at the end of February for the previous calendar year. The IPC/O provides an electronic form and guidance for submitting the statistical report on its website.

Notifying the IPC/O

Gateway CHC abides by the obligation to notify the IPC/O as required by law. Gateway CHC takes guidance from the IPC/O based on its interpretation of the reporting obligations: https://www.ipc.on.ca/health/report-a-privacy-breach/.

Annual statistical reporting to the IPC/O is completed by the Privacy Officer.

Gateway
Community Health Centre

SHARING INFORMATION WITH POLICE GUIDELINES

When can Gateway CHC share information with police?

Sometimes the police contact us for information about our clients. But even confirming to the police that someone is a client of our organization is "personal health information" and Ontario's health privacy law applies. There is a natural tendency for health care providers to want to cooperate with the police and assist them in their investigations. However, this must be balanced against clients' rights to privacy.

So what can Gateway CHC tell police?

- **Refer the Police Officer to the Right Person**

  At Gateway CHC, Management deals with the police. If you are a front-line staff member and you get a call from police or police come to the clinic, please provide the police officer with your supervisor's contact information. Then call your supervisor to let them know the police need assistance. If your supervisor is not available, you can also call the Privacy Officer.

- **In an Emergency - Safety trumps Privacy**

  If Gateway CHC needs to call the police to protect someone from getting hurt, we are allowed to share client information in order to prevent the harm. The law says that is okay. Gateway CHC can also give police health information about a client any time we need to, to reduce or eliminate a significant risk of serious bodily harm. In other words, privacy concerns should never trump sharing information if life and limb are at risk.

Remember:

- If there is time to get advice before calling the police – get advice. Call your supervisor or the administrator on call or the Privacy Officer. Get legal advice or advice from your Professional Association or other source as soon as you can.
- In a true emergency – do your best and share what you need, guided by the principle that safety trumps privacy.
- Only share the minimum amount of information needed in the circumstances
  - It might be enough to say the individual is a client of the organization
  - The police rarely need to know a person's diagnosis.
  - It is usually not necessary to give the police a copy of the client's health record in an emergency. The police have the power to get copies of health records and proper procedure must be followed.

General Information

There are five circumstances in which our organization can disclose identifiable client information to a police officer (and remember, other than in an emergency, Management or the Privacy Officer will normally be the police contact person who decides when and how information will be disclosed):

1. **With the express consent of the client.** In some situations, Gateway CHC will obtain the consent of a client to share information with police. Remember: Implied consent based on the "circle of care" does not apply in the context of disclosing health information to the police, since "circle of care" applies only to health care providers currently providing care to the patient.
2. **For the purpose of eliminating or reducing a significant risk of serious bodily harm.** Health privacy legislation allows us to disclose personal health information to police if we believe on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of bodily harm to a person or group of persons.
3. **In response to a court order or other document requiring us to disclose.** If Gateway CHC receives a court order to disclose information to police, we will disclose it. There are other documents that could also require us to disclose information to the police such as a search warrant, summons or subpoena. Gateway CHC have to read these documents carefully to understand what we are required to do, and by when. If you receive such a document, let Management or the Privacy Officer know or redirect police to that person.

4. **If the police officer is otherwise authorized by law.** Certain legislation authorizes police officers to collect information (such as the *Coroners Act* and the *Mental Health Act*). Gateway CHC will cooperate with police if we are permitted or required by law to share information with them.
5. **If Gateway CHC is otherwise authorized by law.** There are other situations where Gateway CHC has the discretion to involve police officers. If Gateway CHC is permitted by law to share information with police, we may do so; but time permitting, you should check with a supervisor or the Privacy Officer before doing so yourself.

Whenever possible, Gateway CHC will get advice before sharing information with police to ensure we are protecting our clients' rights.