Privacy of Client Information Policy and Procedures

Background
Sherbourne Health Centre (SHC) staff, volunteers and contractors are bound by law and ethics to safeguard your privacy and the confidentiality of your personal information. We believe this trust allows us to provide high quality and safe care to our clients.

This policy has been revised to ensure compliance with the provincial Personal Health Information Protection Act (PHIPA). A separate policy exists for privacy of donor information.

The Privacy Officer is the individual in the organization with overall responsibility for Sherbourne Health Centre’s privacy policies. The office of the Privacy Officer will be filled by the Medical Director. The delegation of responsibility for specific aspects of the policy is as follows:

- CFO/CIO: all issues relating finance, contracts with suppliers and electronic security.
- Human Resources: all issues relating to staff personal and personnel information.

Definitions:

Personal Health Information
Personal health information as defined by PHIPA refers to identifying information about an individual relating to their physical or mental health (including personal and family medical history), the provision of health care to the individual including a plan of service, payments or eligibility for health care, organ and tissue donation and health number.

In addition, any information acquired through involvement with SHC which identifies a client's substitute decision-maker, status, sexual orientation, race, religion, mailing or e-mail address, name, telephone, fax, OHIP, SIN, etc. is considered personal health information and therefore confidential.

Information is identifying if it is foreseeable that it could be used alone or in combination with other information to identify a client.

Health Record
Any written (including, but not limited to electronic) information that contains personal health information about a client constitutes the health record of that client.

Electronic Medical Record (EMR)
Refers to the health record compiled in electronic form by providers of SHC.
Implied Consent
Implied consent is obtained when, given the circumstances of the client, it is reasonable to conclude that the client has by his or her conduct consented to the collection, use or disclosure of the client’s personal health information.

Express Consent
Express consent is obtained when a client explicitly and expressly agrees orally or in writing to the collection, use and disclosure of the client’s personal health information.

1.0 Application

POLICY:
This policy applies to all employees, physicians, volunteers (including the Board of Directors), contracted employees, interpreters, clients, program participants and students who may have access to client information at Sherbourne Health Centre. Staff who are regulated health professionals will be guided by the standards of practice governing their profession. The responsibility for privacy of client health information outlives the professional relationship and continues indefinitely after the provider has ceased to care for the client.

PROCEDURE

1.1 All managers are responsible for ensuring staff in their departments are compliant with the policy.

2.0 Care Delivery and Information Sharing

POLICY:
SHC offers health care within a range of holistic programs and services. Our multi-disciplinary approach requires on-going communication between individual providers and teams. It is important that all clients be aware of what information may be shared between providers and who those providers are. For example, the Child and Family Services Act requires health professionals to report suspected child abuse. A complete listing of situations where a provider is required by law to disclose personal health information is found in Appendix 4.

PROCEDURE:

2.1 Clients will give consent for information to be shared between program teams at SHC by signing an internal referral form, or a staff recording their consent on the internal referral form.
2.2 Consent may also be verbal, in which case it should be recorded in the health record.
2.3 A client should also be made aware of the limits to protection of their privacy. Some legislation requires that staff reveal confidential information to others.
2.4 Clients brought forward to consulting health professionals will remain anonymous when express consent is absent (for example, supervision for mental health). More information about interactions with external agents and consultants can be found in section 15.0.
2.5 All new clients will be informed of the Health Centre’s policy regarding privacy of personal health information through any of the following methods: signage, printed information, and/or personal discussion.

2.6 Sherbourne Health Centre’s Privacy Statement (Appendix 1) will be posted in visible areas throughout the Centre and on Sherbourne Health Centre’s website.

### 3.0 Record Keeping

**POLICY:**

Health records are kept for service planning and monitoring of client progress.

**PROCEDURE:**

3.1 All regulated health care professionals are expected to document in the health record according to the standards of their regulating bodies (e.g. College of Physicians and Surgeons).

3.2 Other staff expected to document in the health record are: counselors, social workers, client resource workers, outreach workers and community health workers.

3.3 Additionally individuals such as the medical secretaries who are providing significant client information are expected to document.

3.4 Only information needed for the care and treatment of clients will be collected and recorded.

3.5 Documentation must be contemporaneous and entries greater than 48 hours after a client interaction must be noted as a ‘Late Entry’ with the date of entry at the top.

### 4.0 Opening and Maintaining a New Health Record

**Policy:**

All new clients to SHC’s family health team will have a new health record created in the electronic medical record.

**Procedure:**

4.1 A new health record is created by the medical secretary staff and designated providers.

4.2 All health records are kept electronically except in specific situations involving satellite sites.

4.3 Information to be recorded on registration must include name, address, and date of birth to comply with legal obligations. OHIP number must be included if applicable.

4.4 Client information is to be checked and updated by medical reception at each visit to ensure its accuracy by both reception staff for demographic and registration information, and by the provider for health and wellness issues.

### 5.0 Access to Client Information

**Policy:**

All access will be on a need to know basis. Staff providing direct services to clients, their managers and their administrative support personnel may have access to client records.
Procedure:

5.1 Any access outside of a need to know basis will be regarded as a serious breach of a client’s privacy and subject to disciplinary measure(s).
5.2 Access will be decided upon by manager/supervisor based on the role of the individual staff.

6.0 Client Access to their Health Record

Policy:
With limited exceptions permitted by law, the client has the right to access all information in their record, including consultation reports marked confidential. However, SHC owns the actual record of the original electronic record and is entitled to control its reproduction.

The request for access to the health record will be processed within a maximum of 30 days. In most cases, SHC will provide access to the record within 5 working days. Any extensions to the 30 day maximum must be documented clearly with the reason given, and a date when the record will be ready.

Procedure:

6.1 Clients will request access to their records in writing using the appropriate form (Appendix 3).
6.2 Clients will be encouraged to specify which part of their health record they are requesting access to (e.g. counselling notes, health bus notes, medical record).
6.3 The request will be received and the identity of the individual confirmed.
6.4 The receptionist/medical secretary will then give the request for the access to the primary provider who will review the request and share it with other providers who have documented in the chart.
6.5 The primary provider will determine if any legal reasons exist to refuse access as per Appendix 2.
6.6 The primary provider will then respond to the request with instructions to either print a copy of the record or to arrange a time to review the chart in person.
6.7 If the client is picking up a copy, they must pick up their records in person and provide identification to the staff releasing the information.
6.8 When a client accesses their original record(s), a staff member must be present to ensure that records are not altered or removed. (Often a provider will want to be present (or should offer to be available) to offer clarification of any part of the record and to offer support.)
6.9 A regulated health care provider may use their discretion in providing personal health information in the context of a clinical visit (e.g. providing a paper copy of blood work at an appointment).

7.0 Refusing Access

Policy:
In limited circumstances, clients may be denied the right of access to their record if this poses a serious risk to themselves or to others. A table of detailed reasons why access may be refused is found in Appendix 2.

Procedure:

7.1 The decision to deny access must be given in writing to the client in accordance with the procedure in Appendix 2.
7.2 The client must be told that he or she has a right to challenge this decision with a complaint to the SHC Privacy Officer, and, if not resolved, to the Provincial Information Privacy Commissioner’s Office.

8.0 Correcting the Clinical Record

Policy:
After reviewing their records, the client may feel that their record is not correct or complete. The client has the right to ask for the record to be corrected. In general, the provider must make the requested correction if the client can demonstrate that the record is not correct or complete for the purposes intended and the client is able to provide the correct information.

Procedure:
8.1 All requests for correcting the clinical chart are to be made in writing and signed by the client.
8.2 The identity of the client is verified by reception or the person receiving the request.
8.3 The primary provider is responsible for assessing the request to correct the record and sharing it with other team members who have documented in the chart.
8.4 The correction should be done by the individual who originally wrote the record.
8.5 The incorrect information should be clearly marked as erroneous and the correct information added.
8.6 The entry must be dated and electronically signed.
8.7 The corrected information must be shared with other providers who are sharing care of the client.
8.8 All requests for chart corrections must be responded to within 30 days.
8.9 The client must be notified in writing if an extension is required with a clear reason for the delay stated and a time frame for completion of the request. The extension can not be longer than 30 days.

9.0 Refusing a request to correct the record

Policy:
If a request is refused for any of the reasons below, the client has a right to make a complaint about the refusal to SHC’s Privacy Officer and, if not resolved, to the Provincial Information and Privacy Commissioner. A professional opinion or observation made in good faith about a client does not need to be corrected.

Staff do not have to correct a record:
- when they do not have sufficient knowledge, expertise and authority to correct the record (this would include the ability to validate the new information being provided),
- if one reasonably believes that the request for correction is frivolous, vexatious or made in bad faith (requests should only be refused for these reasons in the rarest of cases),
- if the client has failed to demonstrate that the record is not correct or complete, or
- if the client has not given you the information you need to make the correction.
Procedure:

9.1 A letter must be sent to the client outlining the reasons for refusal. The client must be told that he or she has a right to challenge this decision with a complaint to the SHC Privacy Officer and, if not resolved, to the Provincial Information Privacy Commissioner's Office.

9.2 The client may make a brief note about the correction refused and have it scanned into the chart. This note must be shared with other providers where relevant.

10.0 Consent to Collect, Use and Disclose PHI
There are two types of consent set out in the PHIPA legislation that pertain to collection, use and disclosure of PHI – implied and express consent. Please see definitions above.

Policy:
When a client requests to be registered to receive health care or other services, their consent can be inferred (considered implied) for the collection, use, and disclosure of their PHI for the provision of the requested health care or the requested services. When a client is aware of a referral to another provider either within or outside SHC, their consent to share information can be inferred (considered implied). However, it is good practice for the referee to explain what information will be shared. When one is referring a client to an internal SHC program, an internal referral form is to be filled out.

Express consent is needed when the information being collected, used or disclosed is not for purposes of providing the requested health care or the requested services. Express consent is necessary for sharing information with another provider in the community for purposes of research or for sharing information with a non-health care provider (e.g. insurance company, employer).

Procedure:

10.1 Express consent can be given in writing, orally, by telephone.
10.2 Express consent must be documented in the client’s health record.

11.0 Withdrawing or Limiting Consent

Policy:
Clients have the right to withdraw their consent to collect, use or disclose their health information at any time. Clients have the right to limit access to parts of their charts if they desire. For example, a client may request that a counsellor not share information with their physician or nurse practitioner or may ask that their HIV status not be shared with another provider.

Procedure:

11.1 Each withdrawal or limitation will be considered on a case-by-case basis with the primary provider, the program manager and/or the Privacy Officer to ensure, among other things, that the withdrawal or limitation does not prevent SHC from fulfilling its legal and ethical obligations.

11.2 It is important to ensure that the client understands the consequences of withdrawing their consent or limiting access to parts of their health record, and this discussion should be documented.
12.0 Release of Client Information to External Agencies/Persons

Policy:

With Consent
Clients have a right to request transfer of their medical records and to expect that the service is done in a timely fashion.

Procedure:
12. 1 The original chart is kept electronically, and the relevant parts are printed out for transfer.
12. 2 The client must give consent for transfer of records by signing a release of information form (a signed letter of request may be acceptable).
12.3 Medical secretaries will collect the signed form or letter.
12.4 The form/letter is passed on to the primary provider to give direction as to the preparation of the document(s) to be printed.
12.5 The medical secretary provides the documents for the primary provider to review prior to transfer.
12.6 A notation is made in the chart by the medical secretary when the information is transferred which includes the date and name to whom it was transferred.
12.7 This release/request letter is then scanned into the chart.
12.8 In certain circumstances it may be acceptable to release information by phone with the client’s verbal consent. Care should be taken to verify the identity of the client and staff should document that the client provided verbal consent.

Policy:

Minors
There is no minimum legal age to give consent to release records. If this competency is not established, the information can only be released through consent of the parent or other legal guardian.

Procedure:
12.9 The provider must ascertain whether the minor is capable of understanding adequately what s/he is directing, and the consequences of the disclosure.

Policy:

Minor Clients of Separated Parents
The Children’s Law Reform Act permits an ‘access parent’ of a minor child to obtain health information about that child. However, many factors may affect the right of an access parent to a child's PHI such as a court order, a separation agreement, a marriage contract, the fact that the parents live outside Ontario and so forth.

Procedure:
12.11 Unless the family situation is clearly understood and consent from all parents/guardians is given, staff should seek guidance from their manager, the Privacy Officer and/or external agency (e.g. Canadian Medical Protective Agency) before disclosing any PHI.

Policy:

Deceased Clients
The executor of a deceased client’s estate is generally entitled to review and have copies of the deceased client’s records, and to give permission for third party viewing.

Procedure:
12.12 Providers are encouraged to get legal advice if there is any uncertainty.

Policy

Incapable Clients
When an individual is incapable of providing consent, a substitute decision maker (such as a relative, spouse, child’s parent, or the Public Guardian and Trustee) may make the decision on that individual’s behalf.

Procedure:
12.13 An individual qualified must determine if a client is incapable before any decision is made with regard to the incapable client’s PHI.
12.14 An assessment of incapability must be noted in the chart.
12.15 Any uncertainty must be addressed with the Privacy Officer or designate.

Policy:

Release without Consent
Client information may be released without consent when required by law or in emergency situations where withholding information could cause serious harm to the client or another person. Legal counsel may be sought. It is important to read the document closely and only comply with what is specifically requested. It will be necessary to determine if all types of information concerning the client are required, or only that of a specific program/service.

Procedure:
12.16 Information directly relevant to the circumstances should be disclosed to the appropriate party, i.e. police, or Children’s Aid.
12.17 If possible, the client should be informed when these situations happen, except when notification could put the client or someone else at risk. The table in Appendix 4 outlines all of the situations where mandatory disclosure must take place.
12.18 A manager is to approve the release of information when there is a subpoena, search warrant or court order.
13.0 Ensuring Privacy And Security Of Personal Health Information

Communication Procedures

Telephone Procedures
13.1 Outgoing phone messages should consist only of a name and phone number, unless the client has consented to have a more detailed message (i.e. has specified to provider, recorded in chart).
13.2 Access to client voicemail messages must be secured (for example, messages picked up at reception and/or in provider’s offices) and must not be audible to other parties when played.

Fax Procedures
13.3 Fax machines for client information must be located in a secure area and use pre-programmed numbers whenever possible to send transmissions.
13.4 All transmissions must be sent with a cover sheet that indicates the information is confidential.
13.5 Reasonable steps will be taken to ensure that health information is received only by a secure fax machine. (For example, this may involve, among other measures, calling first to confirm the fax number and confirm the location is secure.)

E-mail

Policy for Health Care Providers (physicians, nurses, nurse practitioners, medical secretaries):
Email for communication with clients by health care providers is not allowed for the provision of health care services. Only in exceptional circumstances email communication with clients for the provision of health care services may be permissible (for example, hearing impaired clients).

Procedure:
13.6 Staff-to-staff communication of client personal health information via email will either use initials or refer to the client by their chart number.
13.7 In exceptional situations when a health care provider is communicating to a client via email, the client is to sign a consent form (Appendix 8).
13.8 Staff engaging in email communication of personal health information are to review this communication plan with their manager and/or Privacy Officer.
13.9 The signed consent is to be maintained in the client chart.
13.10 Any email communications by health care providers with clients must be copied to the client chart.

Policy for SHC Staff that do not provide health care services:
Email may be used to communicate with clients in programs that do not provide health care if there are administrative, technological and physical precautions to protect personal information (as outlined below).

Procedure:
13.10 Administrative controls:
A. Non-health care providers will be asked to abide by the following rules when using email:
- Email addresses or email content from a client will not be shared with others (including other staff/programs within SHC) unless express consent is obtained.
- Email must not contain personal or identifying information about one client to another client (for example, sending out a group email message to multiple recipients in the “To” field of a message).

B. This entire policy will be reviewed with new staff and on a biannual basis with existing staff.

C. Staff will sign an agreement recognizing they understand and will comply with the ‘Privacy of Client Information Policy’.

D. Each email will contain a confidentiality statement and this statement will direct clients where to get more information regarding the risks of using email.

E. The Privacy Statement will include information for clients regarding email and the Privacy Statement will be posted on the SHC website and throughout the building.

13.11 Technological controls:
A. The server containing email will be protected by a firewall and virus scanning software.
B. Access to email and the server will require passwords (see 15.0).

13.12 Physical control:
A. Any personal or identifying email in hard copy must be stored in locked filing cabinets and be kept in restricted offices.
B. Locked offices will be protected by security services.

Post/Courier Procedures:
13.14 When health information is sent by post or courier, it is placed in a sealed envelope, marked as confidential, and directed to the attention of the authorized recipient.

13.15 If an envelope is translucent and information can be seen through the envelope, staff are to ensure that the information is not visible by using a coversheet, another envelope and/or folding the message.

Physical security procedures:
13.16 All client health related information is to be kept in secure areas such as reception where access is limited to staff members.

13.15 The reception area must be securely locked at all times.
13.16 Filing cabinets and drawers containing PHI must be securely locked when not in use.

13.17 Files/records may be taken to satellite locations only when it is believed to be essential for client care. The records are to remain with the staff responsible for the record(s) at all times. Records are not to be left unattended (even in a locked/area, for example, a locked car/trunk). All records are to be returned the same day.

13.18 Client records are not to be left open or unattended anywhere in the Centre.
13.19 Informal notes should be kept in locked drawers.

13.20 After transferring information to client charts, or when the client information is no longer required, notes are to be shredded.

15.0 Electronic Security
**Policy:**

Sherbourne Health Centre commits to follow provincial guidelines for electronic medical records as set out in Ontario Regulation 114/94, Sections 20 and 21 (Appendix 5).

**Procedure:**

15.1 Access to the health record is on a need-to-know basis.
15.2 User identification (i.e. User ID) and passwords are NEVER to be shared or given out under any circumstances.
15.3 Passwords should not be written down.
15.4 Passwords are changed every ninety (90) days.
15.5 The SHC server (that stores the EMR records and all other data for the organization) must be accessed by a unique user name and password. Exceptions to this are allowed for shared terminals (thin clients) or workstations configured as terminals.
15.6 All computer terminals have the ability to lock the screen and all users must log off or lock the screen when they are leaving their work area unattended (for example, if a client is left unattended to change before a physical exam). Monitors/screens must be situated to prevent clients from seeing the screen.
15.7 All computers will automatically log off users after 1 hour of inactivity.
15.8 All access to EMR data is logged by User ID.
15.9 Access to applications and data is based on the user’s role in the organization and requests outside of the norm are processed based on the approval of the Privacy Officer at SHC or his/her designate.
15.10 Client information must be safeguarded at all times regardless of whether the user is working at SHC, a remote site or at home (for example, logging on remotely must be done in such a way that a screen is not visible to anyone but the authorized staff).

**16.0 Storing Client Information**

**Policy:**

Client records, both written and electronic, are the property of SHC. It is the responsibility of SHC to secure client information against loss, fire, theft, tampering, access, or copying by unauthorized persons.

**Procedure for electronic back up:**

16.1 All data is backed up nightly to tapes.
16.2 The data on these tapes is encrypted and the key to decrypt the data is kept in a secured location.
16.3 Offsite backups are generated weekly and kept in a safety deposit box at the bank used by the organization.

**Procedure for storing and Destroying Client Information**

16.4 All health records compiled at SHC must be kept for 10 years after the date of last entry in a file or 10 years after a client reaches, or would have reached, 18 years of age.
16.5 If the Centre ceases operation, clients will be notified that they have two years in which to transfer their health record to another physician or to claim the record themselves. Two years after notification, the record may be destroyed.
16.6 Information that has been scanned or otherwise entered into the chart may be shredded.
16.7 No original documents of health records compiled in other centres may be destroyed unless in compliance with The Law and Components of Medical Records - Ontario Regulation 114/94, Section 19.

16.8 All paper information with PHI will be physically shredded and destroyed.

16.9 All electronic information must be disposed of securely. This implies physically destroying the hard drive of computers that may have stored personal health information or magnetically erasing the tape.

16.10 All other media (CD, diskettes, tapes, etc) with PHI must be physically destroyed when their use is no longer required.

17.0 Agreement to the Privacy of Client Information Policy and Procedures

All staff (including casual employees), consultants, students, and volunteers (including Board Members) are expected to sign the Confidentiality Statement (Appendix 6) and be aware of, and adhere to, this policy and procedure. The right to privacy of information is to be upheld within SHC and at all satellite locations.

In order to ensure adherence to this policy, staff, students and volunteers are expected to:

- Limit discussion of client personal information to the context of improving client care and/or to protect the safety of others within the health centre, such as when a client is threatening, verbally and/or physically abusive to others, damaging property, etc.
- Avoid discussion of clients in situations where other clients may hear the discussion.
- Respect the privacy of the client phone conversations and make all efforts to not overhear them.
- Raise any observed violations of confidentiality directly with the person making the violation and/or with their manager.

18.0 Ensuring privacy with external agents and contractors:

Policy:

SHC uses external agents and contractors to perform various tasks and roles within the health centre. At times these agents will be involved in collecting, using or disclosing health information. External agents must have permission to collect, use, disclose, retain and dispose of personal health information on SHC’s behalf. External agents must use the information only for the stated purpose and for no other purpose except as permitted or required by any law. External agents must alert SHC if the information they handle is stolen, lost, accessed by unauthorized persons, or used, disclosed or disposed of in an unauthorized manner.

Procedure:

18.1 The checklist in Appendix 7 will be used to guide contract arrangements and monitoring of external agents.

19.0 Fundraising

Policy:

Sherbourne Health Centre commits to not use personal health information for fund raising purposes unless express consent from the client is obtained.
20.0 Complaints

Policy:
Sherbourne Health Centre has a standardized process exists for dealing with client complaints and which is defined in the Complaints Policy.

Procedure:
20.0 Complaints as they pertain to privacy of information will be directed to the Privacy Officer.
20.1 The Privacy Officer may delegate responsibility to another staff member if appropriate.

21.0 Communication of Policy

Policy:
This policy and procedure is to be communicated to every new staff, volunteer and/or contract employee by their line manager. The policy is to be reviewed by all staff either by email, all staff meeting and/or other communications on a biannual basis.

Procedure:
21.1 Each new staff member will receive a copy of this policy from their manager.
21.2 Each staff member will be asked to review this policy every 2 years by their manager.

Reference: OMA/OHA Privacy Toolkit
Appendix 1

General Privacy Statement

Sherbourne Health Centre staff is bound by law and ethics to safeguard your privacy and the confidentiality of your personal information.

This includes:

- Collecting only the information that may be necessary for your care;
- Keeping accurate and up-to-date records;
- Safeguarding the medical records in my possession;
- Sharing information with other health-care providers and organizations on a “need to know” basis where required for your health care;
- Disclosing information to third parties only with your express consent, or when necessary for legal reasons;
- Retaining/destroying records in accordance with the law.

Your request for care from SHC implies consent for our collection, use and disclosure of your personal information for purposes related to your care. As noted above, other purposes require your express consent. You have the right to see your records. You may also obtain copies of your records — please see the receptionist for our procedure for this service. Please speak to your provider if you have any concerns about the accuracy of your records.

If you would like to discuss our privacy policy in more detail, or have specific questions or complaints about how your information is handled, please speak to your provider. If your provider is unable to assist you or to resolve your complaint, please address your question or complaint to Sherbourne Health Centre’s Privacy Officer: The Medical Director, Sherbourne Health Centre, 333 Sherbourne St, Toronto.

Email Privacy Statement:
Sherbourne Health Centre recognizes that email is an important way of communicating. However, because of the privacy risks associated with email, healthcare providers (doctors, nurses, nurse practitioners, medical secretaries) are not able to communicate with clients via email.

Programs that do not provide health care services (e.g. SOY, Parenting Network) may use email to communicate with clients and vice versa.

While Sherbourne Health Centre takes physical, electronic and administrative measures to protect email communication, clients should recognize and accept the risks and conditions associated with
the use of email (as posted on www.sherbourne.on.ca). For a paper copy of these risks and conditions please request this from the Privacy Officer.

RISKS OF USING EMAIL
Transmitting information by email poses several risks that you should be aware of. You should not agree to communicate with the staff by email without understanding and accepting these risks. The risks include, but are not limited to the following:

- The privacy and security of email communication cannot be guaranteed.
- Employers and online services may have a legal right to inspect and keep emails that pass through their system.
- Email is easier to falsify than handwritten or signed hard copies. In addition, it is impossible to verify the true identity of the sender, or to ensure that only the recipient can read the email once it has been sent.
- Emails can introduce viruses into a computer system, and potentially damage or disrupt the computer.
- Email can be forwarded, intercepted, circulated, stored or even changed without the knowledge or permission of the sender or recipient. Email senders can easily misaddress an email, resulting in it being sent to many unintended and unknown recipients.
- Email is indelible. Even after the sender and recipient have deleted their copies of the email, backup copies may exist on a computer or in cyberspace.
- Use of email to discuss sensitive information can increase the risk of such information being disclosed to third parties.
- Email can be used as evidence in court.
- The client waives the encryption requirement, with the full understanding that such waiver increases the risk of violation of the client’s privacy.

CONDITIONS OF USING EMAIL
- The staff and centre will use reasonable means to protect the security and confidentiality of email information sent and received. However, because of the risks outlined above, the staff and sender cannot guarantee the security and confidentiality of email communication and will not be liable for improper disclosure of confidential information that is not the direct result of intentional misconduct of the provider.
## Allowable Reasons for Refusal of Access to the Health Record

<table>
<thead>
<tr>
<th>Reason for Refusal of Access</th>
<th>Follow-Up Notification to Requestor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>State you are refusing the request (in whole or in part) and reason for the refusal</td>
</tr>
<tr>
<td>The record contains quality of care information</td>
<td>×</td>
</tr>
<tr>
<td>The record contains information collected/created to comply with the requirements of a quality assurance program under the <em>Health Professions Procedural Code</em> that is Schedule 2 to the <em>Regulated Health Professions Act</em></td>
<td>×</td>
</tr>
<tr>
<td>The record contains raw data from standardized psychological tests or assessments</td>
<td>×</td>
</tr>
<tr>
<td>The record (or information in the record) is subject to a legal privilege that restricts disclosure to the requestor</td>
<td>×</td>
</tr>
<tr>
<td>Other legislation or court order prohibits disclosure to the requestor</td>
<td>×</td>
</tr>
<tr>
<td>The information in the record was collected/created in anticipation of or use in a proceeding that has not concluded</td>
<td></td>
</tr>
<tr>
<td>Reason for Refusal of Access</td>
<td>Follow-Up Notification to Requestor</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The information in the record was collected/created for an inspection/investigation/similar procedure authorized by law that has not concluded</td>
<td>State you are refusing the request (in whole or in part) and reason for the refusal</td>
</tr>
<tr>
<td>Granting access could reasonably be expected to result in a risk of serious harm to the client or to others (Where this is suspected you may consult a physician or psychologist before deciding to refuse access)</td>
<td>×</td>
</tr>
<tr>
<td>Granting access could lead to the identification of a person who was required by law to provide the information in the record</td>
<td>×</td>
</tr>
<tr>
<td>Granting access could lead to the identification of a person who provided the information in the record in confidence (either explicitly or implicitly) and it is considered appropriate to keep the name of this person confidential</td>
<td>×</td>
</tr>
<tr>
<td>The request for access is frivolous, vexatious or made in bad faith</td>
<td>×</td>
</tr>
<tr>
<td>The identity or authority of the requestor cannot be proven by the requestor</td>
<td>×</td>
</tr>
</tbody>
</table>
Appendix 3

CONSENT FOR VIEWING/RECEIPT OF HEALTH RECORDS

I ___________________________ with chart number ________________________ am

writing to request access to my ___________________________ records.

This access may take the form of a review of the electronic record, or be a printed copy of the record. I
understand that if I request a printed copy of the record, that I may be charged a reasonable fee for
photocopying.

Additionally I understand that access to the record needs to be discussed with my primary care provider(s)
(e.g. counsellor, nurse practitioner or physician), and that a staff member of Sherbourne Health Centre may
choose to be with me when I review the records to answer any questions I may have. If this is the case, an
appointment will be made for me to return and review the records.

I understand that requests to view records can not be processed immediately. A printed copy of the record
requires a minimum of 5 working days to produce. In keeping with provincial guidelines, Sherbourne’s
commitment is to respond to this request within a maximum of 30 days of receipt of this form.

__________________________________

__________________ _______________
Signature        Witness

Date __________________________

__________________________________
## Mandatory Disclosure of Personal Health Information

<table>
<thead>
<tr>
<th>To whom disclosure must be made</th>
<th>What information must be disclosed</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aviation Medical Advisor</td>
<td>Information about flight crew members, air traffic controllers or other aviation licence 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)</td>
<td>Aeronautics Act</td>
</tr>
<tr>
<td>Chief Medical Officer of Health or Medical Officer of Health</td>
<td>Information to diagnose, investigate, prevent, treat or contain communicable diseases</td>
<td>Health Protection and Promotion Act</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Personal Health Information Protection Act</td>
</tr>
<tr>
<td>Chief Medical Officer of Health or a physician designated by the Chief Medical Officer of Health</td>
<td>Information to diagnose, investigate, prevent, treat or contain SARS</td>
<td>Public Hospitals Act</td>
</tr>
<tr>
<td>Children’s Aid Society</td>
<td>Information about a child in need of protection (e.g., abuse or neglect)</td>
<td>Child and Family Services Act</td>
</tr>
<tr>
<td>College of a regulated health care professional</td>
<td>Where there are reasonable grounds to believe a health care professional has sexually abused a patient, details of the allegation, name of the health care professional and name of the allegedly abused patient The patient’s name can only be provided with consent You must also include your name as the individual filing the report.</td>
<td>Regulated Health Professions Act</td>
</tr>
<tr>
<td>To whom disclosure must be made</td>
<td>What information must be disclosed</td>
<td>Authority</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>College of a regulated health care professional</td>
<td>A written report, within 30 days, regarding revocation, suspension, termination or dissolution of a health care professionals’ privileges, employment or practice for reasons of professional misconduct, incapacity or incompetence</td>
<td>Regulated Health Professions Act</td>
</tr>
<tr>
<td>College of Physicians and Surgeons of Ontario</td>
<td>Information about the care or treatment of a patient by the physician under investigation</td>
<td>Public Hospitals Act</td>
</tr>
<tr>
<td>Coroner or designated Police Officer</td>
<td>Facts surrounding the death of an individual in prescribed circumstances (e.g., violence, negligence or malpractice)</td>
<td>Coroners Act</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information about a patient who died while in the hospital after being transferred from a listed facility, institution or home</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information requested for the purpose of an investigation</td>
<td></td>
</tr>
<tr>
<td>Minister of Health and Long-Term Care</td>
<td>Information for data collection, organization and analysis</td>
<td>Public Hospitals Act</td>
</tr>
<tr>
<td>Ontario Health Insurance Plan</td>
<td>Information about the funding of patient services</td>
<td>Public Hospitals Act</td>
</tr>
<tr>
<td>To whom disclosure must be made</td>
<td>What information must be disclosed</td>
<td>Authority</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>Order, warrant, writ, summons or other process issued by an Ontario court</td>
<td>Information outlined on the warrant, summons, etc.</td>
<td><em>Personal Health Information Protection Act</em></td>
</tr>
<tr>
<td>Physician assessor appointed by the Ministry of Health and Long-Term Care</td>
<td>Information to evaluate applications to the Underserviced Area Program</td>
<td><em>Public Hospitals Act</em></td>
</tr>
<tr>
<td>Registrar General</td>
<td>Births and deaths</td>
<td><em>Vital Statistics Act</em></td>
</tr>
<tr>
<td>Registrar of Motor Vehicles</td>
<td>Name, address and condition of a person who has a condition that may make it unsafe for them to drive</td>
<td><em>Highway Traffic Act</em></td>
</tr>
<tr>
<td>Subpoena issued by an Ontario court</td>
<td>Information outlined in the subpoena</td>
<td><em>Personal Health Information Protection Act</em></td>
</tr>
<tr>
<td>Trillium Gift of Life Network</td>
<td>For tissue donations or transplants purposes, notice of the fact that a patient died or is expected to die imminently</td>
<td><em>Trillium Gift of Life Network Act</em></td>
</tr>
<tr>
<td>Workplace Safety and Insurance Board</td>
<td>Information the Board requires about a patient receiving benefits under the <em>Workplace Safety and Insurance Act</em></td>
<td><em>Workplace Safety and Insurance Act</em></td>
</tr>
</tbody>
</table>

Consent must be decided jointly with the Network to determine the need to contact the patient or substitute decision-maker.
Appendix 5

The Law and Electronic Medical Records

Ontario Regulation 114/94, Sections 20 and 21

20. The records required by regulation may be made and maintained in an electronic computer system only if it has the following characteristics:

- The system provides a visual display of the recorded information.
- The system provides a means of access to the record of each patient by the patient’s name and, if the patient has an Ontario health number, by the health number.
- The system is capable of printing the recorded information promptly.
- The system is capable of visually displaying and printing the recorded information for each patient in chronological order.
- The system maintains an audit trail that,
  - records the date and time of each entry of information for each patient,
  - indicates any changes in the recorded information,
  - preserves the original content of the recorded information when changed or updated, and
  - is capable of being printed separately from the recorded information for each patient.
- The system includes a password or otherwise provides reasonable protection against unauthorized access.
- The system automatically backs up files and allows the recovery of backed-up files or otherwise provides reasonable protection against loss of, damage to, and inaccessibility of, information.

21. A member shall make his or her equipment, books, accounts, reports and records relating to his or her medical practice available at reasonable hours for inspection by a person appointed for the purpose under a statute or regulation.
Appendix 6

STATEMENT OF CONFIDENTIALITY

I acknowledge that I have read and understood the Sherbourne Health Centre policies and procedures on privacy, confidentiality and security.

I understand that:

- all confidential and/or personal health information that I have access to or learn through my employment or affiliation with Sherbourne Health Centre is confidential,
- as a condition of my employment or affiliation with Sherbourne Health Centre, I must comply with these policies and procedures, and
- my failure to comply may result in the termination of my employment or affiliation with Sherbourne Health Centre and may also result in legal action being taken against me by Sherbourne Health Centre and others.

I agree that I will not access, use or disclose any confidential and/or personal health information that I learn of or possess because of my affiliation with Sherbourne Health Centre, unless it is necessary for me to do so in order to perform my job responsibilities. I also understand that under no circumstances may confidential and/or personal health information be communicated either within or outside of Sherbourne Health Centre, except to other persons who are authorized by Sherbourne Health Centre to receive such information.

I agree that I will not alter, destroy, copy or interfere with this information, except with authorization and in accordance with the policies and procedures.

I agree to keep any computer access codes (for example, passwords) confidential and secure. I will protect physical access devices (for example, keys and badges) and the confidentiality of any information being accessed.

I will not lend my access codes or devices to anyone, nor will I attempt to use those of others. I understand that access codes come with legal responsibilities and that I am accountable for all work done under these codes. If I have reason to believe that my access codes or devices have been compromised or stolen, I will immediately contact the Sherbourne Health Centre.

_________________________  ______________________  _________________
Name (Please Print)   Signature   Date

_________________________
Position
Appendix 7

CHECKLIST FOR AGENT AGREEMENTS

Bind your agents to:

- name someone to be responsible for privacy compliance,
- only use the information you share with them as needed to fulfill the contract,
- only disclose information you or the law allows,
- put effective administrative, technological and physical safeguards in place to stop theft, loss and unauthorized access, copying, modification, use, disclosure or disposal of information that are at least as rigorous as your own and those offered to the agents’ other clients,
- only give access to subcontractors that you have approved, and only enter into subcontracts that have all of the security provisions contained in your contract with them,
- educate their employees on privacy laws and policies and take reasonable steps to ensure employee compliance through staff training, confidentiality agreements and employee sanctions,
- ensure that employees who are fired or resign return all information and cannot access applications, hardware, software, network and facilities belonging to either you or the agents,
- remind exiting employees of their continued responsibility to maintain the confidentiality of the information,
- use reasonable efforts, including virus protection software, to avoid viruses, worms, back doors, trap doors, time bombs and other malicious software,
- maintain backup security and acceptable business recovery plans (including disaster recovery, data backup and alternate power),
- follow all applicable privacy laws, including the Personal Health Information Privacy Act,
- comply with their own privacy policies,
- share their privacy policy with you and send you any updates or changes made during the term of the contract,
- refer anyone trying to access, correct or complain about their personal health information to your contact person,
- let you inspect their premises and security practices to ensure they are following the law, your contract and privacy policies,
- let you review their internal practices, books and records relating to their use and disclosure of your patients’ information so you can ensure compliance,
- review security regularly and address any threats revealed,
- regularly report on compliance,
- report any security breaches or incidents to you within an agreed time,
- revoke any user’s access if security is breached and on your reasonable request,
• give you a copy of your data when you ask for it,
• securely discard or return any personal health information on your request,
• comply with any sanctions for breaching the contract, including ending the contract or compensating you,
• end the contract for not following it in a significant way,
• return or destroy all information received or created in any form when the contract ends, and where this is not possible, keep the contract’s privacy measures in place to protect the remaining information, and
• never deny you access to information you request because of your late or disputed payment for services.

Your contracts should also include:
• your right to go to court for an order stopping an agent from violating privacy sections of the contract and an acknowledgement that you have been irreparably harmed,
• your remedies for an agent’s breach of the contract, and
• a clause making your agent responsible to you for any costs you pay because of your agent’s failure to sufficiently protect your patients’ information, with insurance to back the clause up.

When sharing personal health information with health information network providers, you must make sure your contract requires them to give you:

• an electronic record of all accesses, uses and disclosures of the information, including the time and source of access, and
• a written assessment of how the services they offer may threaten, make vulnerable or risk the security and integrity of the information, and how they impact privacy.†

† The information set out in bold italicized text is based on draft Regulations that have not yet been finalized.
Appendix 8

Provider-Client Email Communication
Template Consent Form

PROVIDER INFORMATION

Name: ________________________________________________

Address: ________________________________________________

Email: ________________________________________________

RISKS OF USING EMAIL
The provider offers clients the opportunity to communicate by email. Transmitting client information poses several risks of which the client should be aware. The client should not agree to communicate with the provider via email without understanding and accepting these risks. The risks included, but are not limited to the following:

➤ The privacy and security of email communication cannot be guaranteed.
➤ Employers and online services may have a legal right to inspect and keep emails that pass through their system.
➤ Email is easier to falsify than handwritten or signed hard copies. In addition, it is impossible to verify the true identity of the sender, or to ensure that only the recipient can read the email once it has been sent.
➤ Emails can introduce viruses into a computer system, and potentially damage or disrupt the computer.
➤ Email can be forwarded, intercepted, circulate, stored or even changed without the knowledge or permission of the sender or recipient. Email senders can easily misaddress an email, resulting in it being sent to many unintended and unknown recipients.
➤ Email is indelible. Even after the sender and recipient have deleted their copies of the email, back-up copies may exist on a computer or in cyberspace.
➤ Use of email to discuss sensitive information can increase the risk of such information being disclosed to third parties.
➤ Email can be used as evidence in court.
➤ The provider uses encryption software as a security mechanism for email communications. The client waives the encryption requirement, with the full understanding that such waiver increases the risk of violation of the client’s privacy.
CONDITIONS OF USING EMAIL
The provider will use reasonable means to protect the security and confidentiality of email information sent and received. However, because of the risks outlined above, the provider cannot guarantee the security and confidentiality of email communication and will not be liable for improper disclosure of confidential information that is not the direct result of intentional misconduct of the provider. Thus, clients must consent to the use of email for client information. Consent to the use of email includes agreement with the following conditions:

- Emails to or from the client concerning diagnosis or treatment may be printed in full and made part of the client’s medical record. Because they are part of the medical record, other individuals authorized to access the medical record, such as staff and billing personnel, will have access to those emails.
- The provider may forward emails internally to the provider’s staff and to those involved, as necessary, for diagnosis, treatment, reimbursement, health care operations, and other handling. The provider will not, however, forward emails to independent third parties without the client’s prior written consent, except as authorized or required by law.
- Although the provider will endeavour to read and respond promptly to an email from the client, the provider cannot guarantee that any particular email will be read and responded to within any particular period of time. Thus, the client should not use email for medical emergencies or other time-sensitive matters.
- Email communication is not an appropriate substitute for clinical examinations. The client is responsible for following up on the provider’s email and for scheduling appointments where warranted.
- If the client’s email requires or invites a response from the provider and the client has not received a response within a reasonable time period it is the client’s responsibility to follow up to determine whether the intended recipient received the email and when the recipient will respond.
- The client should not use email for communication regarding sensitive medical information, such as sexually transmitted disease, AIDS/HIV, mental health, developmental disability, or substance abuse. Similarly, the provider will not discuss such matters over email.
- The client is responsible for informing the provider of any types of information the client does not want to be sent by email, in addition to those set out in the bullets above. Such information that the client does not want communicated over email includes:

The client can add to or modify this list at any time by notifying the provider in writing.

- The provider is not responsible for information loss due to technical failures.

INSTRUCTIONS FOR COMMUNICATIONS BY EMAIL
To communicate by email, the client shall:

- Limit or avoid using an employer’s computer.
- Inform the provider of any changes in client’s email address.
- Include in the email: the category of the communication in the email’s subject line, for routing purposes (e.g. “prescription renewal”); and the name of the client in the body of the email.
Review the email to make sure it is clear and that all relevant information is provided before sending to the provider.

Inform the provider that the client received the email.

Take precautions to persevere the confidentiality of emails, such as using screen savers and safeguarding computer passwords.

Withdraw consent only by email or written communication to the provider.

Should the client require immediate assistance, or if the client’s condition appears serious or rapidly worsens, the client should not rely on email. Rather, the client should call the provider’s office for consultation or an appointment, visit the provider’s office or take other measures as appropriate.

CLIENT ACKNOWLEDGEMENT AND AGREEMENT
I acknowledge that I have read and fully understand this consent form. I understand the risks associated with the communication of email between the provider and me, and consent to the conditions outline herein, as well as any other instructions that the provider may impose to communicate with clients by email. I acknowledge the provider’s right to, upon the provision of written notice, withdraw the option of communicating through email. Any questions I may have had were answered.

Client name: ________________________________________________________________

Client address: ______________________________________________________________

Client email: ________________________________________________________________

Client signature __________________________________________ Date: ________________

Witness signature __________________________________________ Date: ________________