Section Title	**Policy and Procedures for All Staff**
Policy Title:	**Privacy of Client Information Policy and Procedures**
Approved by:	**Senior Management Team**
Date Last Approved:	**March 29, 2004**
Date Revised:	**September 2014**
Next Revision Date:	**September 2017**

PRIVACY OF CLIENT INFORMATION POLICY AND PROCEDURES

Background

Sherbourne Health Centre (SHC) staff, volunteers and contractors are bound by law and ethics to safeguard client privacy and the confidentiality of personal information.

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 as follows:

- Chief Financial Officer (CFO)/Chief Operating Officer (COO): All issues relating finance, contracts with suppliers and electronic security
- Human Resources: All issues relating to staff personal and employment information.

Definitions:

Personal Health Information

Personal health information (PHI) 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, substitute decision-makers, organ and tissue donation information and health number.

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

Identifying Information

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

Health Record

A health record is 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)

An electronic medical record (EMR) is a computer-based medical record. It is the record clinicians maintain on their own patients, and which detail demographics, medical and drug history, and diagnostic information such as laboratory results and findings from diagnostic imaging which are received directly from Ontario Lab Information Systems, community labs and hospital reports via hospital report manager. It is often integrated with other software that manages activities such as billing and scheduling.

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.

Expressed Consent
Expressed 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, volunteers (including the Board of Directors), contracted employees, interpreters, clients, program participants and students who may have access to personal information at SHC. Staff who are regulated health professionals will be guided by the standards of practice governing their profession unless SHC applies a higher standard, in which case SHC policy will prevail. The responsibility for the protection of personal information, including personal 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 (including students and volunteers) in their departments are aware and 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 listing of situations where a provider is required by law to disclose personal health information is found in Appendix 4. In addition, SHC or a provider may be required to provide information as a result of a production order, subpoena or search warrant.

PROCEDURE

2.1 Clients will be informed that SHC provides interdisciplinary team care and information when appropriate may be shared by all pertinent members of client's circle of care.

2.2 Providers will document this verbal consent by entering a check in box of client's intake form entitled "circle of care".

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 All new clients will be informed of this policy regarding privacy of personal health information through any of the following methods: signage, printed information, and/or personal discussion.

2.5 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 primarily for service planning and monitoring of client progress. They may also be used for risk assessments and quality of care analysis in appropriate circumstances when applicable law permits that use.

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) and SHC policy and standards.

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 completed at the time of the visit 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 secretary 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 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.

5.3 Management may access records for the purposes of investigating client feedback/complaints and care/services received at SHC, and/or interactions with SHC staff/providers.

5.4 Privacy audits will be conducted by the Health Information and Systems Manager and reviewed with the Privacy Officer on a quarterly basis.

5.5 Any suspicious activity in a client's chart will be followed up with staff and staff's director to ensure charts are not being accessed inappropriately.

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 business 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. Clients should be encouraged to use 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. counseling notes, health bus notes, etc.).

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 Ontario Information and 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. The correct information is added and saved.
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 cannot 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 Commissioners. 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 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 expressed 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 service. 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 a good practice for the referee to explain what information will be shared. When one is referring a client to an internal SHC program (e.g. dietician, diabetes program, counseling), 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 counselor not share information with their physician or nurse practitioner.

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 Restricting Access to Client's EMR (Chart)

POLICY

Primary health care is provided by a SHC Interdisciplinary team. Members of the Client Care Team may change from time to time. During an Intake process, clients sign their acknowledgement and/or give verbal consent to providers within the 'circle of care' to access Clients' Electronic Medical Records on a need to know basis. If there are extenuating circumstances that make it necessary to apply restrictions, limiting access to only certain providers, the request will be processed the following way:

PROCEDURE:

12.1 Client will submit their concerns to their providers in writing (Appendix 9).
12.2 Request will be assessed by a provider, the Program Director, the Health Information and Systems Manager and Privacy Officer.
12.3 When a request is accepted and a signed statement is received, the request will be processed and the chart will have restricted access to certain providers as requested by client.
12.4 The signed form will be scanned into the chart.
12.5 In Electronic Medical Records program (Accuro), there is the ability to restrict the following information to only certain users:

- chart information of all clinical encounters
- clinical documents
- medical history
- medication history

There is not the ability to restrict access to the following:

- client demographics
- the functionality of booking appointments

13.0 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

13.1 The original chart is kept electronically, and the relevant parts are printed out for transfer.
13.2 The client must give consent for transfer of records by signing a release of information form (a signed letter of request may be acceptable).
13.3 Medical secretaries will collect the signed form or letter.
13.4 The form/letter is passed on to the primary provider to give direction as to the preparation of the document(s) to be printed.
13.5 The medical secretary provides the documents for the primary provider to review prior to transfer.
13.6 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.
13.7 This release/request letter is then scanned into the chart.
13.8 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 identify of the client and staff should document that the client provided verbal consent.

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.

PROCUDURE

13.9 The provider must ascertain whether the minor is capable of understanding adequately what they are directing, and the consequences of the disclosure.

Minor Clients of Separated Parents
The *Children's Law Reform Act* permits an 'access parent' of a minor child to obtain health information about the 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

13.10 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 Protection Agency) before disclosing any PHI.

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

13.11 Providers are encouraged to get legal advice if there is any uncertainty.

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

13.12 A qualified individual must determine if a client is incapable before any decision is made with regard to the incapable client's PHI.
13.13 An assessment of incapacity must be noted in the chart.
13.14 Any uncertainty must be addressed with the Privacy Officer or designate.

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

13.15 Information directly relevant to the circumstances should be disclosed to the appropriate party, i.e. police, or Children's Aid.
13.16 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 of the situations where mandatory disclosure must take place.
13.17 A manager is to approve the release of information when there is a subpoena, search warrant or court order.

14.0 Ensuring Privacy and Security of Personal Health Information

PROCEDURE for Telephone and Fax Communications

Telephone Procedures

14.1 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.
14.2 Access to client voicemail messages must be secured (for example, messages picked up at reception and/or in provider's office) and must not be audible to other parties when played.
14.3 Use of Smartphones/PDAs for client PHI recording/communication should follow the "no identifiers" rule, using client's initials or chart number only.

Fax Procedures

14.4 Fax machines for client information must be located in a secure area and use pre-programmed numbers whenever possible to send transmissions.
14.5 All transmissions must be sent with a cover sheet that indicates the information is confidential. Digitally faxed Rx and Referrals, requisitions have disclaimers generated from EMR.
14.6 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/Text

POLICY for Health Care Providers (physicians, nurses, nurse practitioners, medical secretaries):

Email or text messages for communication with clients by health care providers are 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 email be permissible (for example, hearing impaired clients).

PROCEDURE

14.7 Staff-to-staff communication of client personal health information via email will either use initials or refer to the client by their chart number.
14.8 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).

14.9 Staff engaging in email communication of personal health information are to review this communication plan with their manager and/or Privacy Officer.

14.10 The signed consent is to be maintained in the client chart.

14.11 Any email communications by health care providers with clients must be copied to the client chart.

14.12 Staff are not permitted to email "screen grabs" of client's PHI.

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

14.13 Administrative Controls:

A. Non-health care providers are expected to abide by the following rules when using email:
   a. 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.
   b. Email must not contain personal or identifying 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 bi-annual basis with existing staff at All Staff meetings, lunch and learns, in combination with email reminders.

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 a statement stating that SHC discourages the transmission of personal health information by 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.

14.14 Technological Controls:

See Section 15.

14.15 Physical Control:

A. Any personal or identifying email in hard copy must be stored in locked filling cabinets and be kept in restricted offices after it is scanned or pasted to a client's chart.

B. Locked offices will be protected by security services.

14.16 Post/Courier Procedures

A. 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.

B. 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.

14.17 Physical Security Procedures:

A. All client health related information is to be kept in secure areas such as reception where access is limited to staff members.

B. The reception area must be securely locked at all times.

C. Filling cabinets and drawers containing PHI must be securely locked when not in use.

D. 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.

E. Health records are not to be left open or unattended anywhere in the centre. EMRs must be locked when not in use (e.g. Alt +F12 to lock the Accuro EMR screen).

F. Informal notes should be kept in locked drawers.
G. After transferring information to client charts, or when the client information is no longer required, notes are to be shredded. Hard copies of patient clinical documents received from external healthcare organizations and the forms with client signatures are scanned in the charts and kept for six months in a secured place. It is shredded after six months.

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 display will automatically turn off after 10 minutes of inactivity and computers will go to sleep after 30 minutes of inactivity by default.
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).

COO Responsibilities

POLICY

The COO is responsible for developing and employing technical security policies and procedures to prevent unauthorized access, use, modification, destruction or disclosure of personal information, including personal health information.

PROCEDURE

15.11 The COO will develop policies and procedures appropriate to the sensitivity of the personal information.
15.12 Without limiting the foregoing, (a) Servers hosting personal information or email will be protected by a firewall and virus scanning software; and (b) access to email and applications containing personal information must be protected by unique user IDs and passwords.
15.13 The COO will periodically review with the CEO and Chief Privacy Officer the policies and procedures used to protect personal information.
15.14 The COO will at least annually review with the Board the policies and procedures used to protect personal health information.

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. Electronic back ups of the EHR will be run on a daily basis and on a monthly basis the tape will be stored off site in a secure location.

16.4 The electronic back ups will be tested for integrity on a regular basis.

PROCEDURE for Storing and Destroying Client Information

16.5 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.

16.6 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.

16.7 Information that has been scanned or otherwise entered into the chart may be shredded.

16.8 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.

16.9 All paper information with PHI will be physically shredded when destroyed.

16.10 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.

16.11 All other media (CD rom, 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

POLICY

All staff (including contract and 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.

PROCEDURE

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 and must sign a Contract Services Agreement which includes a comprehensive privacy appendix. 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. Contract Services Agreement includes a comprehensive privacy appendix.

PROCEDURE

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

19.0 Fundraising

POLICY

SHC commits to not use personal health information for fund raising purposes unless explicit consent from the client is obtained.

20.0 Reporting of Unauthorized Access, Use, Modification, Destruction or Disclosure of Personal Information

POLICY

SHC shall take steps to contain and investigate any suspected unauthorized access, use, modification, destruction, or disclosure of personal information (a "breach"). All breaches will be reported in accordance with applicable laws.

PROCEDURE

20.1 A person who becomes aware of or suspects conditions that could give rise to a breach shall report the breach to the Chief Privacy Officer and, in the absence of the Chief Privacy Officer, any one of the COO, CFO or Director of Human Resources/Corporate Communications ("HR Director").

20.2 The Chief Privacy Officer or the other responsible person listed in section 20.1 who is notified shall convene a team as soon as possible consisting of appropriate personnel to contain the breach. In addition, such team shall investigate and report to the Chief Privacy Officer regarding (a) the extent of the breach, (b) the nature of the personal information that may have been exposed, (c) the risk of harm as a result of the breach, and (d) the root causes of the breach.

20.3 The Chief Privacy Officer or delegate shall report all breaches to the CEO. The CEO, the Chief Privacy Officer or delegate shall report all breaches to the Board.

20.4 The Chief Privacy Officer or delegate shall make any mandatory breach reports to oversight agencies as required under applicable law. SHC conduct individual breach notification if required under applicable law.

21.0 Complaints

POLICY

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

PROCEDURE

20.1 Complaints as they pertain to privacy of information will be directed to the Privacy Officer.

20.2 The Privacy Officer may request the assistance of or delegate responsibility to another staff member if appropriate to investigate or to resolve the complaint.

22.0 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 bi-annual basis.

PROCEDURE

22.1 Each new staff member will receive a copy of this policy

22.2 Each staff member will be asked to review this policy every 2 years by their manager.

Reference: OMA/OHA Privacy Toolkit

Appendix 1

SHERBOURNE
Health Centre

Privacy Statement

Sherbourne Health Centre (SHC) staff takes steps to safeguard your privacy and the confidentiality of your personal information.

This includes:

- Identifying the purposes for collecting your personal information;
- Collecting only the information that may be necessary to fulfill those purposes;
- Keeping accurate and up-to-date records;
- Safeguarding personal information in our custody or 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 securely and in compliance with applicable laws or regulations.

What we collect
We collect your personal information directly from you in most cases. However, we may also collect personal information from other professionals, persons acting on your behalf, or others if you have provided your consent or the law permits.

If you are a client, the personal information we may collect will include your contact information, medical history, records of the care you received during prior visits to SHC or other clinics or hospitals. Your request for care from SHC implies consent for our collection, use and disclosure of your personal information for purposes related to your care.

We also collect personal information that you provide to us if you become a donor or a volunteer, if you make an application for employment, or if you participate in one of our programs.

How we use and disclose your personal information
If you are a client, we use and disclose your personal health information to provide you with care and for related purposes. These include:

- To provide you with care;
- To communicate with other professionals to whom you are referred for care or consultation;
- To process payments for your treatment (from OHIP, WSIB and others);
- To manage our programs and services, including conducting risk management activities and quality improvements;
- To conduct research, provide education to health professionals, and to conduct patient surveys;
- To perform other activities consistent with the operation of a health care centre;
- Other purposes for which you consent or are specifically permitted or required by applicable law.

We also use and disclose personal information for other programs and services. For example, we may use your personal information to solicit and process donations, to enroll you in one of our programs at your request, to manage our volunteer programs in which you participate, and for other purposes that are identified at the time of collection or prior to at the time of the use or disclosure of your personal information.

In some cases, we may be required by law to disclose your personal information. We may also disclose your personal information if it is reasonably necessary to protect you, SHC, SHC staff, volunteers or clients, or other individuals, and such disclosure is permitted by applicable laws.

Access and Correction
You have the right to access the personal information we have collected or created about you. If you are a client, this includes 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.

Questions and Complaints
If you receive health care services and would like to discuss our privacy policy in more detail, or have specific questions or complaints about how your personal information is handled, please speak to your provider.

If, having discussed your concerns with your provider, your complaint has not been satisfactorily resolved, please address your question or complaint to Sherbourne Health Centre's Privacy Officer:

The Medical Director
Sherbourne Health Centre
333 Sherbourne Street
Toronto, ON M5A 2S5

Inactive clients and members of the public may also address general questions, concerns or complaints to the Privacy Officer.

Email and Website Privacy Statement
SHC 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. If a client wishes to be contacted via email, they must sign a written agreement that they understand the risk of using email with respect to the protection/privacy of their personal health information. (See consent form Appendix 8).

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

While SHC 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.

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 may be falsified. In addition, it is difficult 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 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 these 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 SHC 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 unless it is the direct result of intentional misconduct of the provider.

Website

When you visit or interact with us through our website, we and our service providers may use technologies that automatically collect information about how you access, navigate and leave our website. For example, we will collect information on what other website you came to before visiting the Sites, what browser type and operating system you are using, the internet protocol (IP) address you are accessing the website from, the pages you are navigating through and what website you go to after visiting our website. In general, we do not associate this type of information with other personal information about you except in the case of an investigation into our website security. Our website uses analytics services, including Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses cookies to help the website analyze how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage.

Appendix 2

Allowable Reasons for Refusal of Access to the Health Record

Reason for Refusal of Access	**Follow-Up Notification to Requestor**	
	State you are refusing the request (in whole or in part) and reason for the refusal	**State you are refusing to confirm or deny the existence of any record**
The record contains quality of care information	✕	
The record contains information collected/created to comply with the requirements of a quality assurance program under the *Health Professions Procedural Code* that is Schedule 2 to the *Regulated Health Professions Act*	✕	
The record contains raw data from standardized psychological tests or assessments	✕	
The record (or information in the record) is subject to a legal privilege that restricts disclosure to the requestor	✕	
Other legislation or court order prohibits disclosure to the requestor	✕	
The information in the record was collected/created in anticipation of or use in a proceeding that has not concluded		✕
The information in the record was collected/created for an inspection/investigation/similar procedure authorized by law that has not concluded		✕

Reason for Refusal of Access	Follow-Up Notification to Requestor	
	State you are refusing the request (in whole or in part) and reason for the refusal	**State you are refusing to confirm or deny the existence of any record**
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)		✕
Granting access could lead to the identification of a person who was required by law to provide the information in the record		✕
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		✕
The request for access is frivolous, vexatious or made in bad faith	✕	
The identity or authority of the requestor cannot be proven by the requestor	✕	

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 cannot 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

Appendix 4

Mandatory Disclosure of Personal Health Information

To whom disclosure must be made	What information must be disclosed	Authority
Aviation Medical Advisor	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)	***Aeronautics Act***
Chief Medical Officer of Health or Medical Officer of Health	Information to diagnose, investigate, prevent, treat or contain communicable diseases	***Health Protection and Promotion Act*** ***Personal Health Information Protection Act***
Chief Medical Officer of Health or Medical Officer of Health or a physician designated by the Chief Medical Officer of Health	Information to diagnose, investigate, prevent, treat or contain SARS	***Public Hospitals Act***
Children's Aid Society	Information about a child in need of protection (e.g., abuse or neglect)	***Child and Family Services Act***
College of a regulated health care professional	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.	***Regulated Health Professions Act***
College of a regulated health care professional	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	***Regulated Health Professions Act***

To whom disclosure must be made	What information must be disclosed	Authority
College of Physicians and Surgeons of Ontario	Information about the care or treatment of a patient by the physician under investigation	***Public Hospitals Act*** Notice must be given to the Chief of Staff and the administrator of the hospital
Coroner or designated Police Officer	Facts surrounding the death of an individual in prescribed circumstances (e.g., violence, negligence or malpractice) Information about a patient who died while in the hospital after being transferred from a listed facility, institution or home Information requested for the purpose of an investigation	***Coroners Act***
Minister of Health and Long-Term Care	Information for data collection, organization and analysis	***Public Hospitals Act***
Ontario Health Insurance Plan	Information about the funding of patient services	***Public Hospitals Act***
Order, warrant, writ, summons or other process issued by an Ontario court	Information outlined on the warrant, summons, etc.	***Personal Health Information Protection Act***
Physician assessor appointed by the Ministry of Health and Long-Term Care	Information to evaluate applications to the Underserviced Area Program	***Public Hospitals Act***
Registrar General	Births and deaths	***Vital Statistics Act***
Registrar of Motor Vehicles	Name, address and condition of a person who has a condition that may make it unsafe for them to drive	***Highway Traffic Act***
Subpoena issued by an Ontario court	Information outlined in the subpoena	***Personal Health Information Protection Act***

To whom disclosure must be made	What information must be disclosed	Authority
Trillium Gift of Life Network	For tissue donations or transplants purposes, notice of the fact that a patient died or is expected to die imminently	***Trillium Gift of Life Network Act*** Consent must be decided jointly with the Network to determine the need to contact the patient or substitute decision-maker
Workplace Safety and Insurance Board	Information the Board requires about a patient receiving benefits under the *Workplace Safety and Insurance Act*	***Workplace Safety and Insurance Act***

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) **Position**

_____ _____

Signature **Date**

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 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.

Health Information Network Providers
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.

Appendix 8

PROVIDER-CLIENT EMAIL COMMUNICATION
Template Consent Form

PROVIDER INFORAMTION

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 may be falsified. In addition, it is difficult 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 provider uses encryption software as a security mechanism for email communications. The client waives these 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 inform 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 endeavor 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. 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 preserve 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 worsened, 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***

Appendix 9

SHERBOURNE
Health Centre

REQUEST FORM FOR RESTRICTED ACCESS TO MEDICAL RECORDS

Sherbourne Health Centre provides primary care with an interdisciplinary team. Members of your care team will have access to your medical records to provide care. The members of your care team may change from time to time.

You may use this form to request restrictions on access to your medical records. **However, if the personal health information in the records is reasonably necessary for the provision of health care, your care team may not be able to provide you with that health care.**

Please explain what personal health information you do not want used or disclosed by specific care providers at Sherbourne Health Centre. Your request will be assessed and processed by your care provider, the Program Director, the Health Information and Systems Manager, and the Privacy Officer, who may request additional information or who may discuss the implications of your request with you.

Please describe the restrictions you want on access to your electronic medical record and the reasons for your request (add pages if necessary):

_____

_____

_____

_____

READ CAREFULLY: I acknowledge and agree that restricting access to my personal health information may result in Sherbourne Health Centre being unable to provide me the best possible health care. If the personal health information in the records is reasonably necessary for the provision of health care, I acknowledge and agree that my care team may not be able to provide me with care.

_____ _____

Full Name (Please print) **Chart Number**

_____ _____

Signature **Date**