

ST. MICHAEL'S HOSPITAL FOUNDATION PERSONAL INFORMATION PRIVACY POLICY

Goal, Standards and Scope

St. Michael's Hospital Foundation ("the Foundation") is committed to protecting the privacy of personal information (of all individuals, including employees) on an ongoing basis. To realize this goal, the Foundation collects, use(s) and disclose(s) personal data in accordance with relevant data protection legislation, public expectation and internationally accepted fair information principles.

In formulating its approach to the protection of privacy, the Foundation policy is consistent with the 10 principles of fair information practice, as laid out in the *Canadian Standards Association Model Code for the Protection of Personal Information*—Canada's standard for fair information practice. As well, in its approach, the Foundation complies with all applicable laws and established guidelines for charitable organizations.

This policy covers all personal information under the control of the Foundation regardless of what medium is used to store, move or copy that data. The following documents each of the 10 CSA principles of fair information practice and the Foundation's practices related to each principle. At the point of approval of this policy, the Foundation is working towards developing a full range of procedures necessary to implement its privacy program. The goal for completion of a fully operational privacy program is early 2004.

Accountability

The Foundation is responsible for the information —particularly personal information —under its control. This includes all personal information that has been transferred to a third party for processing.

The Foundation has a designated individual, known as the Privacy Officer, who is accountable for the Foundation's compliance with its Privacy Policy. The Privacy Officer's name and contact information is made available to the public. The current designate is Pat Hetherington, who can be reached at 416-864-6060 ext. 6164. The Privacy Officer reports to the President of the Foundation.

While the Privacy Officer is tasked with the day-to-day operation of the Foundation's Privacy Program, the President of the Foundation oversees the Foundation's overall compliance with this policy.

In addition, each person who works for the Foundation - whether employee, volunteer or board member - has an individual responsibility to comply with the Foundation's Privacy Policy. Each of these individuals receives education and

training about the Foundation's privacy policies and procedures and is expect to take personal responsibility for the following:

- monitoring and addressing any condition that may threaten the confidentiality or security of personal information;
- reporting possible problems and improvements in information confidentiality and security to the Privacy Officer;
- receiving and reporting complaints to the Privacy Officer;
- helping to solve problems and implement improvements;
- keeping abreast of the Foundation policies and related procedures.

The Privacy Officer has established a Foundation Privacy Working Group with representation from each of the Foundation program areas. The Group meets on an ongoing basis to assess privacy-related issues.

Identifying Purposes

Personal information will be collected in a manner that is consistent with the agreed upon purpose and will only be used by those with a need to know in fulfilling that purpose. At the time of collection, the Foundation will identify the purpose for which personal information is collected. The primary purpose is to raise funds for St. Michael's Hospital through the following activities:

- Major Gifts
- Special Events
- Annual Fund Donations
- Planned Giving

If collected personal data is to be used for a purpose not previously identified, this additional purpose will be identified to the individual prior to use. Unless this new purpose is required by law, the individual's consent regarding this new purpose is required.

Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, unless required by law.

- Consent to use selected items of personal data for Foundation purposes, among other purposes, is sought by the Hospital, as part of its routine collection of patient data

- An individual may withdraw consent previously given at any time. An opt-out option is available on printed and electronic publications. If consent is withdrawn, the Foundation will comply with this request.

Limiting Collection

The collection of personal information will be limited to that which is necessary for the purposes identified by the organization. Information will be collected by fair and lawful means.

- Anyone collecting personal information on behalf of the Foundation should be able to provide an explanation to the individual of the purpose for which the data is being collected.
- The Foundation will not collect personal information indiscriminately. Both the amount and type of personal information collected must be the minimum amount necessary to satisfy that purpose. As much as possible, personal information will be collected directly from the individual.
- The Foundation does not collect personal health information, other than that which has been volunteered directly by the individual.

Limiting Use, Disclosure and Retention

Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. If an individual does consent to collection, use and disclosure of his or her personal information for an identified purpose, then that information will be retained for no longer than is required to fulfill that purpose, unless additional retention is required by law. When the retention period has expired, all copies of the personal information under the control of the Foundation will be destroyed, erased or made anonymous, according to procedure.

- The Foundation does not sell, rent or trade personal information with third parties.
- Information provided by individuals to make an online donation through the Foundation's website, is used only for the purposes of the specific transaction. Donations are processed through a third party and the security and privacy policies of the third party are available by clicking on the "Security and Privacy Policy" icon on the online donation form.
- In the process of fulfilling the identified purpose – for which consent has been given – the Foundation may disclose personal information to non-employees of the Foundation who have a need-to-know in the course of fulfilling the purpose. In each case, the recipient of personal data has

signed an agreement with the Foundation, agreeing to hold the information in confidence and use it only for the agreed upon purpose. In any other case, explicit consent must be obtained from the individual before personal information is disclosed to any third party.

- Personal information will be retained only as long as necessary for the fulfillment of the identified purpose.
- The Foundation is developing retention and destruction schedules for all personal information. These guidelines will include minimum and maximum retention periods. Personal information must be retained long enough to allow the individual access to the information collected for an identified purpose. The Foundation is also subject to legislative requirements with respect to retention periods.
- The Foundation will designate custodians for personal information in all formats. Designated custodians of records containing personal information are responsible to ensure that assigned records are stored safely and confidentially for the appropriate retention period. When retention periods for specific records expire, the designated custodian is responsible for ensuring the records are destroyed. The method of destruction must leave no recoverable trace of personal information.

Accuracy of Personal Information

Personal information will be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

- As much as possible, personal data will be collected directly from the individual.
- The extent to which personal information will be accurate, complete and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information will be sufficiently accurate, complete and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about an individual.
- Personal information that is used on an ongoing basis, including information that is disclosed to third parties, will generally be accurate and up-to-date, unless limits to the requirements for accuracy are clearly set out.
- Individuals may modify or change any personal information previously provided to the Foundation by contacting the Privacy Officer.

Ensuring Safeguards for Personal Information

Security safeguards appropriate to the sensitivity of the information will protect personal information. Access to personal data (regardless of format) will be strictly monitored with controls, appropriate to the sensitivity of the data, in place to prevent against loss, theft, unauthorized access, disclosure and copying of data.

- Every person who may access personal information must sign a confidentiality agreement, prior to being granted access to that data. As a condition of employment, the Foundation requires that the new employee sign the Foundation Confidentiality Agreement. Volunteers are also required to sign an agreement.
- Personal information access will be audited from time to time by the Privacy Officer to ensure that actual access conforms to authorized access.
- The nature of safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information and the method of storage. A higher level of protection will apply to more sensitive information.
- Methods of protection will include:
 - 1) Physical Measures: For example, locked filing cabinets and restricted access to offices;
 - 2) Organizational Measures: For example, limited access on a “need-to-know” basis, and
 - 3) Technological Measures: For example, the use of passwords, encryption and audits.
- Care will be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

Openness

The Foundation will make readily available to individuals specific information about its policies and practices relating to the management of personal information.

- This publicly-available information will include:
 - 1) Name and contact information for the Foundation Privacy Officer for the purpose of questions and complaints.
 - 2) How access is sought
 - 3) A description of the type of personal information held by the Foundation including a general account of its use.
 - 4) A copy of the following documents: St. Michael's Hospital Foundation Personal Information Privacy Policy; Privacy Statement and Retention Schedules
 - 5) Description of personal information made available to related organizations
- This publicly-available information may be dispersed through a variety of means, including: brochures, mailings, signage, online or via phone.
- Printed versions of any of these documents may be requested in writing to the Privacy Officer

Individual Access

Upon request, an individual will be informed of the existence, use, and disclosure of his or her personal information and will be given access to that information. An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, the Foundation may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

- Each individual has the right to view his or her own records, except if doing so would disclose personal data of another individual.
- The individual may also amend his or her own records, provided the original record remains available for reference.

- Upon request, the Foundation will inform an individual whether or not it holds personal information about that individual. The Foundation will seek to indicate the source of this information and will allow the individual access to same. In addition, the Foundation will provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.
- An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided will only be used for this purpose.
- The Foundation will respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information will be provided or made available in a form that is generally understandable. For example, if the Foundation has used abbreviations or codes to record information, an explanation will be provided.
- When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the Foundation will amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information will be transmitted to third parties having access to the information in question.
- When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge will be recorded by the Foundation and addressed by the Privacy Officer.

Challenging Compliance

An individual will be able to address a challenge concerning compliance with this policy to the Foundation Privacy Officer.

- The Foundation will establish a process to address complaints about the privacy, confidentiality and/or security of personal information,
- The complaint procedure will be easily accessible and simple to use. The Foundation will make this procedure known to those who lodge complaints.
- The Privacy Officer will investigate all complaints. If a complaint is found to be justified, appropriate measures will be taken, including amending policies and procedures where required.
- Complaints that cannot be resolved by the Privacy Officer will be referred to the President of the Foundation. If a resolution can still not be reached, a challenge will further be considered by the Manager of Information Security for St. Michael's Hospital.

Incident Recognition, Response, Reporting and Follow-Up

Everyone who works with the Foundation has an obligation to ensure confidentiality of personal information is preserved at all times.

- Anyone observing a breach of confidentiality or a potential breach should report the details as quickly as possible to the Foundation Privacy Officer. Forms will be available for reporting such activity. The Privacy Officer will discuss the issue with the President of the Foundation.
- If there is violation of the agreement, disciplinary action, up to and including termination of employment or association with the Foundation, may be taken.

Staff and Volunteer Education

Through orientation sessions and periodic educational sessions, SMHF ensures everyone who works with SMHF or on its behalf has a good understanding of privacy policies and the supporting procedures.

Routine Assessment of Systems and Processes

Information systems and work processes are routinely assessed to confirm that privacy of personal data is protected, and that only authorized people with a need to know have access to personal data.

- Whenever significant changes are proposed or undertaken for systems or work processes, and whenever substantial external services and products are evaluated or contracted to assist with information management, a privacy impact assessment will be conducted.

Audits and Reviews

The Foundation Privacy Working Group will periodically conduct internal reviews and external audits of its privacy policies and practices, with a view to maintaining and improving their effectiveness, and complying with the relevant legislation.

APPROVED BY FOUNDATION BOARD FEBRUARY 17, 2004

Saved as: S:\PRIVACY - MASTER FOLDER\Privacy Policy\Final – Approved February 17, 2004