

APPENDIX A

The 10 Guiding Principles

1. Accountability for Personal Information

The Ottawa Hospital (TOH) is responsible for personal information under its custody or control. Accountability for TOH's compliance with the principles rests with the Chief Privacy Officer, even though other individuals within the hospital are also responsible for the day-to-day collection and processing of personal health information.

Employees/agents of TOH are responsible to report any breach of this policy. If there is a known breach of confidentiality, the infraction must be reported to the Hospital's Chief Privacy Officer and to the person responsible for protecting the personal information (e.g. manager, director, etc.).

Violation of this policy is grounds for disciplinary action up to and including dismissal. Physicians and residents breaching their duty of privacy and confidentiality as outlined in this policy may be subject to suspension or termination of privileges.

TOH shall use affiliation agreements or other means to provide a comparable level of protection while personal health information is being processed or accessed by a third party.

TOH is responsible for information that has been transferred to a third party for processing. TOH will use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

TOH will implement corporate policies and practices to give effect to this policy, These include:

- Procedures to protect personal health and employee information. Many mechanisms exist to protect employee and patient information such as encrypted electronic records and locking paper records. Awareness about the importance of securing information would be achieved through orientation & training.
- Procedures to receive and respond to complaints and enquiries. Patient complaints would be received and responded through Patient Relations and the Chief Privacy Officer's office.
- Education and communication to employees about TOH's policies and procedures.
- Providing oversight and leadership with respect to privacy and protecting information through the office of the Chief Privacy Officer. The Office oversees all activities related to the development, implementation, maintenance of, and adherence to the Hospital's policies and procedures covering the privacy, confidentiality and security of personal health information. This includes access to personal health information by patients and their families, as well as amendments to personal health information in compliance with current and upcoming federal and provincial laws and the Hospital's information privacy practices.

2. Identifying Purposes for the Collection of Personal Information

At or before the time personal information is collected, TOH will identify the purposes for which personal information is collected. The primary purposes are:

- to provide clinical care to patients of TOH;
- to monitor and evaluate the quality of care and the outcomes resulting from that care;
- to assess resource utilization in the delivery of care;
- to plan for the development and delivery of care and services across the City of Ottawa and Eastern Ontario;
- to support and promote research and education;
- to document patterns of illness to support prevention programs and early disease detection;
- to support and promote fundraising for TOH; and
- to meet legal and regulatory requirements.

TOH shall only collect the information it needs to fulfill these purposes.

The identified purposes shall be specified, at or before the time of direct collection, to the individual from whom the personal health information is collected. Depending on the way in which the personal health information is collected, this will be done orally or in writing. An admission form, for example, may give notice of the purposes. A patient who presents for treatment is also giving implicit consent for the use of his or her personal information for authorized purposes.

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use.

Persons collecting personal health information on behalf of TOH shall be able to explain to individuals the purpose for which the information is being collected.

3. Consent for the Collection, Use, and Disclosure of Personal Information

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

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. If TOH does not have a direct relationship with the individual, it may not be able to seek consent.

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, TOH will seek this consent at the time of collection. In certain circumstances, this consent may be sought after the information has been collected but before use (for example, when TOH wants to use information for a purpose not previously identified).

The principle requires "knowledge and consent". TOH will make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

TOH will not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

The form of the consent sought by TOH may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, TOH will take into account the sensitivity of medical and health information.

In obtaining consent, the reasonable expectations of the individual are also relevant. In this case, TOH can assume that the individual's request for treatment constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to TOH would be given to a company selling health-care products.

The way in which TOH seeks consent may vary, depending on the circumstances and the type of information collected. TOH will generally seek express consent when the information is likely to be considered sensitive (e.g., genetic testing). Implied consent would generally be appropriate when the information is less sensitive. An authorized representative (such as a legal guardian or a person having power of attorney) for care can also give consent.

Individuals can give express consent in many ways. For example:

- An admission form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
- A check-off box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

NOTE – OACIS is used by partner organizations, there is no means at this time to meet an individual's request to allow internal use, but prevent affiliate organizations from viewing this information.

- Consent may be given orally when information is collected over the telephone, or
- Consent may be given at the time that individuals use a health service.

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. TOH will inform the individual of the implications of such withdrawal.

4. Limiting Collection of Personal Information

Information will be collected by fair and lawful means.

TOH shall not collect personal health information by misleading or deceiving individuals about the purpose for which information is being collected.

5. Limiting Use, Disclosure, and Retention of Personal Information

Limiting Use and Disclosure:

Personal health 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. When personal health information is to be used for new purposes, this policy will be updated to reflect these changes.

Access to confidential information will be limited to only those employees authorized to hold, view or handle such information for their current job duties. Access is to be determined by the employee's direct supervisor.

Personal information is to be maintained in the strictest of confidence and is not to be shared with unauthorized persons. For example, employees/agents must avoid engaging in discussions about personal information in public areas such as hallways, elevators, cafeterias, etc.

Audits are conducted on the Hospital's electronic records. Limitations are placed on users to ensure that they only have access to information they require to do their job..

Authorized access to a computer system requires user sign-on, logon-id and password. There are different layers of access, each requiring a unique Logon ID and Password. These include:

- Remote access via Virtual Private Network (VPN) or modem and secure phone line (for more information, see the Remote Access policy);
- The Ottawa Hospital network (for more information, see the Network Services policy);
- Computer Applications (for more information, see the Computer Applications policy).

Each layer has its own rules in terms of password length, etc. however, the basic security principles apply to all.

An electronic signature (combination of logon-id and confidential password) establishes authorship and validity of a statement, order, document, report, or record by an electronic means.

It is the responsibility of each user to ensure that his or her password is secure. Users are prohibited from sharing (lending or borrowing) their password on any system. Passwords must: never be recorded in any way (written down or stored in a user's computer); never be entered via a batch file or other automated process (the password must be manually entered each time); and never be used to attempt to assume another person's identity. If there is reason to believe a password has been compromised, it is to be changed immediately followed by immediate notification to one's supervisor.

If an employee or agent is in doubt as to whether or not to disclose personal information, the employee shall consult with his or her immediate supervisor, or contact the Hospital's Chief Privacy Officer.

Employees/agents may not disclose personal information to legal authorities such as police officers or lawyers without the consent of the data subject (e.g. patient, his or her substitute decision-maker, or employee) unless there is a valid search warrant or subpoena issued. The search warrant or subpoena should specify the type of information requested.

All proposed research uses of personal health information are subject to review by a properly constituted Research Ethics Board prior to consideration by TOH.

Limiting Retention:

Personal information will be retained only as long as necessary for the fulfilment of those purposes. In OACIS records are kept forever, there is no provision, function or policy re. Deleting information.

TOH will develop guidelines and implement procedures with respect to the retention of personal information. Personal health information used for research purposes will be in accordance with TOH's

requirements for clinical research. TOH is subject to legislative requirements with respect to retention periods.

Personal health information that is no longer required to fulfil the identified purposes will be shredded, erased, incinerated or made anonymous. TOH has developed guidelines to govern the destruction of personal information.

6. Ensuring Accuracy of Personal Information

Personal health information should be as accurate, complete, and up-to-date as possible.

This is to minimize the possibility that inappropriate information may be used to make a decision about the individual.

TOH shall not routinely update personal health information, unless such a process is necessary to fulfil the purposes for which the information was collected, such as updating addresses.

Personal health information that is used on an ongoing basis, including information that is disclosed to third parties, shall generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

7. Ensuring Safeguards for Personal Information

Security safeguards appropriate to the sensitivity of the information will protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. TOH will protect personal information regardless of the format in which it is held.

The nature of the 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 safeguard more sensitive information, such as financial and health records.

All information assets and services that are utilized by the Hospital's network are covered by this policy. The policy applies equally to servers, peripheral equipment, and desktop computers within or connecting to the Hospital network. Network resources include data, information, software, hardware, telecommunications equipment, and facilities (including an individual's home, if working remotely). This policy applies to all individuals utilizing or connecting to any aspect of the Hospital network including employees, contractors, physicians, clinics, other institutions.

The methods of protection will include:

- Physical measures, for example, locked filing cabinets and restricted access to offices;
- Administrative measures, for example, limiting access on a "need-to-know" basis, and
- Technical measures, for example, the use of passwords, encryption, and audits.

The Information Systems / Information Technology (I.S./I.T.) Department is responsible to:

- ensure the network environment has appropriate security commensurate with sensitivity, criticality, etc;
- provide a secure, managed firewall;

- provide reasonable protection from security breaches such as virus attacks and hackers;
- ensure that security is cost-effective based on a cost versus risk ratio, or that is necessary to meet with applicable mandates;
- Management is responsible for approving IT requirements for their staff and ensuring practices to secure computerized data;
- ensure individual accountability for the appropriate use of information technology;
- conduct regular audits of the network environment,
- inform all end-users of the auditing functions and capabilities;
- provide a secure environment with authorized physical access to the Hospital's data processing facilities.

TOH will make its employees aware of the importance of maintaining the confidentiality of personal information. As a condition of employment, all new TOH employees/agents (e.g. employee, clinician, physician, allied health, volunteer, researcher, student, consultant, vendor or contractor) must sign the TOH commitment to maintain confidentiality. In addition, TOH employees/agents must implement the following safeguards to protect personal information:

- ensure any locally stored data are replicated to a corporate repository for proper backup and archiving (data backups that are not stored on I.S./I.T. servers are the responsibility of the end-user and must be executed a minimum of weekly).
- ensure data on drives/media are protected and secured using available corporate encryption mechanisms and software products.
- ensure that commercially sensitive information, including email, is encrypted wherever necessary.
- take reasonable care to ensure that electronic viruses are not imported into the Hospital environment (e.g. employees/agents should not run executable files downloaded or received via the Internet).

Confidential information is not to be left in written form or displayed on computer terminals in areas or locations where unauthorized individuals may access it. Confidential information is not to be left unattended where there is no one to receive the information (e.g. fax machines).

Confidential information is to be stored in the least publicly accessible areas in secure cabinets that can be easily locked. The keys to these cabinets must also be kept in a secure area away from the cabinets themselves.

Transportation of information is to be done in a secure manner. (see ADM III 111 Transmission of Patient Information By Facsimile).

Any information that is lost and found, which is deemed to be confidential, should be returned immediately to the appropriate area to which it belongs.

Reproduction of any personal information should be limited and in accordance with Bill 31 and should not interfere with the integrity of the information. Employees/agents reproducing documents are responsible for ensuring that the documents are not left behind and that any discarded copies are to be

disposed of according to the procedures and processes outlined in the Confidential Waste Disposal Policy.

Care will be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information. (For more information, see the Confidential Waste Disposal Policy).

8. Openness about Personal Information Policies and Practices

TOH will make available to individuals specific information about its policies and practices relating to the management of personal information under its custody or control.

Individuals will be able to acquire information about its policies and practices without unreasonable effort. This information will be made available in a form that is generally understandable.

The information made available will include:

- The name or title, and the address, of the person(s) who is accountable for TOH's policies and practices and to whom complaints or inquiries can be forwarded;
- The means of gaining access to personal health information under TOH's custody or control;
- A description of the type of personal health information held by TOH, including a general account of its use;
- A copy of any brochures or other information that explain TOH's policies, standards or codes;
- A list of personal health information that may be made available to other agencies and health care professionals, Medical Officers of Health, researchers and The Ottawa Hospital Foundation.

TOH may make information on its policies and practices available in a variety of ways. For example, TOH will make notices or brochures available in its places of business, and may mail information to its clients on request, as well as provide on-line access to information about its policies and practices with respect to the management of personal information.

9. Individual Access to Own Personal Information

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, TOH may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will 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.

Upon request, TOH will inform an individual whether or not TOH holds personal information about the individual. TOH will seek to indicate the source of this information and will allow the individual access to this information. However, TOH may choose to make sensitive medical information available through a medical practitioner. In addition, TOH 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 TOH to provide an account of the existence, use, and disclosure of personal information. The information provided will only be used for this purpose.

In providing an account of third parties to which it has disclosed personal information about an individual, TOH will attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, TOH will provide a list of the organizations to which it may have disclosed information about the individual.

TOH will respond to an individual's request within a reasonable time and at a given cost to the individual. The requested information will be provided or made available in a form that is generally understandable. For example, if TOH uses abbreviations or codes to record information, an explanation will be provided.

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, TOH 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, TOH will record the substance of the unresolved challenge. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question. The challenge will be recorded and filed within the Office of The Chief Privacy Officer.

10. Challenging Compliance with TOH's Privacy Policies and Practices

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

TOH will put procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.

TOH will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist.

TOH will investigate all complaints. If a complaint is found to be justified, TOH will take appropriate measures, including, if necessary, amending its policies and practices.