HANOVER & DISTRICT HOSPITAL

**ADMINISTRATION POLICIES AND PROCEDURES MANUAL**

| | | | |
|---|---|---|---|
| Policy Covering: | **PRIVACY POLICY** | | |
| Effective Date:<br>Reviewed Date: | January 2020<br>January 2020 | Section: General Administration | Policy # **ADM 1-80** |
| Prepared By: | Registration & Privacy Officer | Supersedes Policy #/Dated:<br>ADM 1-80/August 2017 | Page 1 of 9 |
| Cross Reference: | ADM 9-15 – Information Services Security Policy | Related Forms: | H-10 Privacy Notice to Patients |
| Reviewed by: | Manager of Health Records/Registration & Privacy Officer | | |
| Issued By: | President & CEO | | |

**PURPOSE:**

As a personal health information custodian (HIC) under the *Personal Health Information Protection Act*, 2004 (*PHIPA*), the Hanover & District Hospital (HDH) staff and physicians are committed and responsible for ensuring the protection of personal information of its patients, employees, medical staff, students, volunteers, and agents to the fullest extent possible. This policy includes all personal information which is the property of the Hospital in all formats, including oral, hard copy and electronic. The Hospital will ensure that personal information is maintained private, confidential, and secure. Security includes technical, physical and administrative safeguards.

Collection, use, access or disclosure of personal information of other individuals by staff is strictly on a basis of informed consent, and on a legitimate need-to-know basis to perform job duties. Staff are accountable for maintaining privacy and confidentiality, as outlined in this policy and related procedures, of all personal information during and after employment, agency relationship or affiliation with the Hospital.

This privacy policy does not replace any statutory, common law, ethical, or contractual obligations that are in place with respect to how the Hospitals collect, use, and disclose personal information.

Hanover and District Hospital, South Bruce Grey Health Centre, Grey Bruce Health Services, Muskoka Algonquin Healthcare, and Orillia Solders' Memorial Hospital have implemented a shared electronic health record. Hanover and District Hospital and the Hanover Medical Associates share personal health information. To the extent that personal health information is collected, used, disclosed and retained within shared databases, Hanover and District Hospital recognizes that it has both independent and joint obligations with respect to fair information practices.

**POLICY:**

This policy and its related procedures establish the rules about the manner in which personal information may be collected, used or disclosed, retained, amended, destroyed and includes the following requirements:

- Obtaining informed and knowledgeable consent for the collection, use and disclosure of personal information;
- Safeguarding and treating all personal information as confidential;
- Providing an individual access to his/her personal information, as well as ensuring the right to correct errors;
- Giving an individual the right to instruct the Hospital not to share any part of his/her personal information with others;
- Establishing clear guidelines for the use and disclosure of personal information for fundraising and research purposes;
- Identifying the exceptions to the above requirements;
- Ensuring accountability by granting an individual the right to complain to the Information and Privacy Commissioner of Ontario and/or the Federal Privacy Commissioner; and
- Establishing remedies for breaches in privacy that may occur.

HDH is responsible for personal information under its control and is committed to a high standard of privacy for its information practices. All Hospital policies and procedures relating to the collection, retention, release, security, and destruction of personal information are developed in consideration of the following ten principles based on the CSA Model Code, the national privacy standard for Canada.

***Principle 1 - Accountability for Personal Information***

HDH is responsible for personal information under its control and has designated an individual as Privacy Officer who is accountable for compliance at HDH using the following principles:

1. Accountability for the Hanover and District Hospital's compliance with the policy rests with the President and Chief Executive Officer, even though other individuals within the hospital are responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the Hospital may act on behalf of the President and Chief Executive Officer such as the Manager of Health Records/Privacy Officer.

2. The name of the Privacy Leadership designated by HDH to oversee compliance with these principles is a matter of public record.

3. HDH is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. HDH will use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4. HDH will:
   - Implement policies and procedures to protect personal information, including information relating to patients, staff and agents.
   - Establish policies and procedures to receive and respond to complaints and inquiries.
   - Train and communicate to staff and agents, information about the Hanover and District Hospital's privacy policies and practices.

- Develop plans and communicate to the public and key hospital stakeholders' information to explain HDH's privacy policies and procedures.

***Principle 2 – Identifying for the Collection of Personal Information***

At or before the time personal information is collected, the Hanover and District Hospital will identify the purposes for which personal information is collected.

1. HDH collects personal information for the purposes of:
   - Direct patient care;
   - Administration and management of the health care system;
   - Research, teaching and statistics, fundraising; and
   - Complying with legal and regulatory requirements.
2. HDH collects personal information once the purposes have been identified.
3. HDH will specify the identified purposes at or before the time of collection (if possible) to the individual from whom the personal information is collected. Notice of the purposes for which the information is collected shall be displayed in the Registration areas at the Hanover and District Hospital. A patient who presents for treatment and receives an explanation is also giving implied consent for the use of his or her personal information for authorized purposes. If individuals wish to have more information regarding the purposes and procedures of the collection, use, and disclosure of their information, a patient notice is also available. Refer to *Form H-10* – Privacy Notice to Patients Handout.
4. 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. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.
5. Persons collecting personal information will be able to explain to individuals the purposes for which the information is being collected.

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

The knowledge and consent of the individual are required for collection, use and 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. In these circumstances, the Hanover and District Hospital should seek consent from a substitute decision maker, where possible. In addition, if the Hanover and District Hospital does not have a direct relationship with the individual, it may not be possible to seek consent.

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

2. HDH 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.

3. HDH 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.

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

5. In obtaining consent, the reasonable expectations of the individual are also relevant. HDH can assume that an 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 HDH would be given to a company selling health-care products.

6. The way in which HDH seek consent may vary, depending on the circumstances and the type of information collected. The Hanover and District Hospital will generally seek express consent when the information is likely to be considered sensitive (i.e. genetic testing). Implied consent would generally be appropriate when the information is less sensitive. HDH shall seek consent from an authorized representative such as a substitute decision maker if the patient is not capable of giving or refusing consent.

7. Individuals can give 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;
    - Consent may be given orally when information is collected over the telephone; or
    - Consent may be given at any time that individuals use a health service.

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

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

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

1. HDH will not collect personal information indiscriminately. Both the amount and the type of information collected will be limited to that which is necessary to fulfill the purposes identified.

2. HDH will collect information through fair and lawful means and convey to the individual(s) the purpose for which the information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

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

HDH will not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information will be retained only as long as necessary for the fulfillment of those purposes.

1. If using information for a new purpose, HDH will document this purpose.

2. HDH will develop guidelines and implement procedures with respect to the retention of personal information. These guidelines will include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual will be retained long enough to allow the individual access to the information after the decision has been made. Retention guidelines will be based on the directives outlined in the Public Hospitals Act (Reg 965).

3. HDH will develop guidelines and implement procedures to govern the destruction of personal information in accordance with applicable legislative requirements.

***Principle 6 – Ensuring 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.

1. The extent to which personal information will be accurate, complete and up-to-date will depend upon 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 the individual.

2. HDH will update personal information only when necessary to fulfill the purposes for which the information was collected.

3. 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 requirement for accuracy are clearly set out.

***Principle 7 – Ensuring Safeguards for Personal Information***

Personal information will be protected by security safeguards appropriate to the sensitivity of the information.

1. The security safeguards will protect personal information against loss, theft, unauthorized access, disclosure, copying, use, or modification. HDH will protect information regardless of the format in which it is held.

2. 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 records of personal health information.

3. The methods of protection will include:
   - Physical measures, for example, locked filing cabinets and restricted access to offices;
   - Organization measures, for example, limiting access on a "need-to-know" basis; and
   - Technological measures, for example, the use of passwords, encryption and audits.

4. HDH will make its employees aware of the importance of maintaining the confidentiality of personal information. As a condition of employment, appointment, or agency, all hospital staff and agents must sign the Hanover and District Hospital Confidentiality Agreement annually. In addition, those with access to electronic health records must sign individual user agreements (*Administrative Policy #ADM 9-15*).

5. Care will be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

***Principle 8 – Openness about Privacy Policy***

HDH will make readily available to individuals specific information about their policies and practices relating to the management of personal information.

1. HDH will be open about its policies and procedures with respect to the management of personal information. Individuals will be able to acquire information about their policies and practices without unreasonable effort. This information will be made available in a form that is generally understandable.

2. The information made available will include:
   - The name, title, and address of the person(s) who is accountable for HDH's policies and procedures and to whom complaints or inquiries can be forwarded;
   - The means of gaining access to personal information held by HDH;
   - A description of the type of person information held by HDH, including a general account of its use;
   - A copy of any brochures or other information that explains HDH's policies, standards or codes; and
   - What personal information is made available to related organizations

3. HDH will make information on their policies and procedures available in a variety of ways to address varied information needs and to ensure accessibility to information: for example, HDH may choose to make brochures available in their place of business, mail information to their clients, post signs, provide online access, or through the Internet and Intranet.

***Principle 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, HDH may not be able to provide access to all the personal information they hold 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 proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

1. Upon request, the HDH will inform an individual whether or not they hold personal information about the individual. HDH will seek to indicate the source of this information and will allow the individual access to this information. However, they may choose to make sensitive health information available through a medical practitioner. In addition, HDH 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.

2. An individual will be required to provide sufficient information to permit HDH to provide an account of the existence, use, and disclosure of personal information. The information provided will only be used for this purpose.

3. In providing an account of third parties to which they have disclosed personal information about an individual, HDH will attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which they have actually disclosed information about the individual, the Hanover and District Hospital will provide a list of the organizations to which they may have disclosed information about the individual.

4. HDH will respond to an individual's request within a reasonable time and at a reasonable cost to the individual. Fees will be established on a cost recovery basis. The requested information will be provided or made available in a form that is generally understandable. For example, if HDH use abbreviations or codes to record information, an explanation will be provided.

5. When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, HDH will amend the information as required, in accordance with professional standards of practice and for records of personal health information, the provisions of the Personal Health Information Protection Act. Depending upon the nature of the information challenged, amendment may involve the correction, deletion, or addition of information.

Information contained within health records will not be deleted, but rather, the original must be maintained, with any amendments or corrections being made in a transparent manner. Where appropriate, the amended information will be transmitted to third parties having access to the information in question.

6. When a challenge is not resolved to the satisfaction of the individual, HDH 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.

***Principle 10 – Challenging Compliance with the Privacy Policy***

An individual will be able to challenge compliance with this policy with the President and Chief Executive Officer.

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

2. HDH will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures including complaints to the Information and Privacy Commissioner of Ontario. A range of those procedures may exist.

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

**DEFINITIONS:**

**Agent** – a person who acts, with the authorization of the organization, for or on behalf of the organization in exercising powers or performing duties with respect to personal information for the purposes of the organization, and not the agent's own purposes, whether or not employed by the organization or remunerated. Agents may include volunteers, students, physicians, consultants, nurses, vendors and contractors.

**Conditional Consent** – a person's consent to the collection, use or disclosure of personal health information on which the patient has placed a restriction

**Disclose** – release or make personal health information available to another person, organization or health information custodian; it does not mean to use the information.

**Health Information Custodian** – a person or organization who has custody or control of personal health information as a result of or in connection with performing the person's/organization's/duties/work as prescribed under PHIPA (i.e. health care practitioner, pharmacist, hospital, long term care home, laboratory, ambulance services).

**Identifying Information** – any information that identifies an individual or that one could reasonably foresee might be used either on its own or with other information to identify an individual.

**Information Practices** – A health information custodians' policies concerning when, how, and why the health information custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and the administrative, technological and physical safeguards and practices maintained to protect personal health information.

**Patients** – includes inpatients, outpatients, residents and clients.

**Personal Health Information** – identifying information about an individual in oral or recorded form, if the information:

a) Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;
b) Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;
c) Is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual;
d) Related to payments or eligibility for health care in respect of the individual;
e) Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part of bodily substance;
f) Is the individual's health number; or
g) Identifies an individual's substitute decision-maker.

**Personal Information** – information about an identifiable individual, but does not include the name, title or business address or telephone number of a staff member of an organization. Personal information includes personal health information.

**Record** – an information record in any form or media, including written, printed, photographic or electronic form, but excluding computer programs and other mechanisms that produce a record.

**Security** – the physical, technological and administrative protective measures and techniques that are designed to ensure that personal health information remains confidential, available and uncompromised. This includes measures such as encryption, passwords, and firewalls designed to prevent unauthorized access to information, to protect the integrity of computing resources and to limit the potential damage that can be caused by unauthorized access.

**Use** – to handle or deal with personal health information but does not mean to disclose personal health information.

**REFERENCES:**


1. *Personal Information Protection and Electronic Documents Act (Canada)*
2. *Personal Health Information Protection Act, 2004 (Canada)*
3. Hospital Tool Kit: Guide to the Ontario Personal Health Information Protection Act, 2004
4. Privacy Policy, London Health Sciences Centre, 2005.