



## Statement of Information Practices

### **Personal Health Information Protection Act (PHIPA)**

PHIPA is a provincial legislation that governs the collection, use and sharing of personal health information. It is based on ten principles that doctors, hospitals, community health care organizations, and other health practicing facilities must follow when collecting, using and sharing personal health information. Woodstock Hospital has established a privacy program based on these principles.

### **Principle 1 - Accountability for Personal Information/Personal Health Information**

The hospital is responsible for personal information/personal health information under its control and has a designated individual (Privacy Officer) who is accountable for compliance at the hospital. Woodstock Hospital is complying by implementing policies and procedures to protect personal information/personal health information, including information relating to patients, staff, and agents; adhering to policies and procedures when receiving and responding to complaints and inquiries; training and communicating to staff and agents information about privacy policies and practices; developing plans and communicating to our patients, families, members of the public and key hospital stakeholders.

### **Principle 2 - Identifying Purposes for the Collection of Personal Information/Personal Health Information**

The hospital will identify the purposes for which personal information/personal health information is collected at or before the time of collection. These purposes will be conveyed by means of posters, brochures, web sites and by direct contact with the Privacy Office. Primarily, personal information/personal health information is used to deliver patient care, for administration, in research, teaching, statistics, and to meet legal and regulatory requirements. Patients imply consent when they present for treatment and receive an explanation. Unless a new purpose is legally required, consent must be obtained before the information can be used.

### **Principle 3 - Consent for Collection, Use, and Disclosure of Personal Information/Personal Health Information**

An individual's knowledge and consent is required to collect, use, or disclose personal information/personal health information. The form of consent – express or implied – and the way it is sought – in writing or orally – may vary depending upon the circumstances and sensitivity of the information. Consent may be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice. Personal information/personal health 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.

### **Principle 4 - Limiting Collection of Personal Information/Personal Health Information**

Only information necessary for the purposes identified may be collected, by fair and lawful means.

### **Principle 5 - Limiting Use, Disclosure, and Retention of Personal Information/Personal Health Information**

Personal information/personal health information may be used only for the purposes for which it was collected, except with consent or as required by law. The hospital will document any new purpose and may require consent from the individual. The information is retained only as long as necessary, and destroyed in accordance with legislation, hospital policies, guidelines and procedures.



# WOODSTOCK HOSPITAL

## **Principle 6 - Ensuring Accuracy of Personal Information/Personal Health Information**

The hospital will make every effort to ensure the information it holds is accurate, complete and up-to-date. Individuals have the right to challenge the accuracy of the information.

## **Principle 7 - Ensuring Safeguards for Personal Information/Personal Health Information**

The hospital applies security safeguards appropriate to the sensitivity of personal information/personal health information to aim to protect it against loss, theft, unauthorized access, disclosure, copying, use, or modification, regardless of its format. Protection may include physical measures (ie, locked filing cabinets and restricted access), organizational measures (limiting access on a "need-to-know" basis), and technological measures (use of passwords, encryption and audits). Hospital staff and agents will be required to sign a confidentiality agreement as a condition of employment, appointment, or agency. Those with access to electronic health records must sign individual user agreements.

## **Principle 8 - Openness About Personal Information/Personal Health Information Policies and Practices**

The hospital makes information about its privacy policies and practices readily available, in a form that is generally understandable. This will include:

- contact information for the hospital's Privacy Office, to which complaints or inquiries can be forwarded;
- means of gaining access to personal information/personal health information held by the hospital;
- a description of the type of personal information/personal health information held by the hospital,
- including a general explanation of its use;
- brochures or other information explaining the hospital's policies, standards, or codes, and
- what personal information/personal health information is made available to related organizations.

## **Principle 9 - Individual Access to Own Personal Information/Personal Health Information**

Upon request, within a reasonable time and at a reasonable cost, an individual will be informed of the existence, of his or her personal information/personal health information and will be given access to it. They can challenge its accuracy and completeness and have it amended as appropriate.

Exceptions to access will be limited and specific, with reasons provided upon request. This may include information that is prohibitively costly to provide; refers to other individuals; cannot be disclosed for legal, security, or proprietary reasons, or is subject to solicitor-client or litigation privilege.

An individual must provide sufficient information to permit the hospital to identify the existence of personal information/personal health information, including details of third-party recipients.

## **Principle 10 - Challenging Compliance with the Hospitals' Privacy Policies and Practices**

An individual will be able to address a challenge concerning compliance with this policy to the Chief Executive Officer or Privacy Officer. The hospital 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/personal health information. The hospital will investigate all complaints. If a complaint is justified, the hospital will take appropriate measures, including, if necessary, amending their policies and practices.