WOMEN'S COLLEGE HOSPITAL
Health care for women | REVOLUTIONIZED

Administrative Policy Manual

Title: Privacy and Security of Personal Health Information

Women's College Hospital		**Policy No:**	1.20.002
Title	Privacy and Security of Personal Health Information	**Original:** (mm/dd/yyyy)	10/01/2004
Category	Administrative	**Reviewed:** (mm/dd/yyyy)	03/16/2016
Sub-category	Privacy and Information Security	**Revised:** (mm/dd/yyyy)	04/22/2013 01/13/2015
Issued by:	Privacy Office		
Approved by:	Executive Team		

Policy Statement:

Privacy is governed by the Ontario *Personal Health Information Protection Act* (PHIPA), a law that establishes rules governing the collection, use and disclosure of personal health information. As a health information custodian, Women's College Hospital (WCH) and its staff, physicians, volunteers and students are responsible for ensuring that the personal health information of our patients is managed with respect and confidentiality.

The purpose of this policy is to assert WCH"s commitment to the protection of personal health information from theft, loss and unauthorized access, copying, modification, use and disclosure. This policy addresses issues of collection, access, use and disclosure of personal health information.

In formulating its approach to protection of privacy, WCH has these objectives:

- To comply with legislation – the *Personal Health Information Protection Act, 2004* (PHIPA), the *Public Hospitals Act*, the *Mental Health Act* and any other applicable legislation.
- To adhere to the principles of fair information practice, as laid out in the Canadian Standards Association Model Code for the Protection of Personal Information.
- To support the delivery of high quality patient care.
- To reflect established, relevant standards and guidelines including:
    - standards and guidelines from Accreditation Canada;
    - standards and guidelines from the Canadian Health Information Management Association (CHIMA)

Definition:

Agent – PHIPA defines an agent to include any person who is authorized by a health information custodian to perform services or activities on the custodian's behalf and for the purposes of that custodian.

An agent may include an individual or company those contracts with, is employed by or volunteers for a health information custodian and, as a result, may have access to personal health information.

In such cases, the custodian is permitted to authorize the agent to handle or deal with personal health information on its behalf so long as the agent complies with PHIPA and adopts the information practices and policies of the custodian.

Examples of agents of WCH include, but are not limited to: employees, physicians, volunteers, students, residents, fellows, consultants, researchers, and vendors.

Capable – means mentally capable and "capacity" has a corresponding meaning and refers to the ability of a person to consent to the collection, use or disclosure of personal health information. A person is able to consent if he or she is able to understand the information that is relevant to deciding whether to consent to a collection, use or disclosure and to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing consent.

Circle of Care – The "circle of care" is not a defined term under PHIPA. It is a term of reference used to describe health information custodians and their authorized agents who are permitted to rely on an individual's implied consent when collecting, using, disclosing or handling personal health information for the purpose of providing direct health care.

For example, in a hospital, the circle of care includes: the attending physician and the health care team (e.g. physicians, residents, nurses, technicians, health disciplines and employees assigned to the patient or providing support in the provision of care to the patient) who have direct responsibilities of providing care to the individual.

Collection – means the process of gathering, acquiring, receiving or obtaining personal health information whether directly from the patient, or from other sources such as tests, images, samples, specimens or from other health care providers.

Confidentiality – means the obligation to protect someone's personal health information, to maintain the privacy of the information and not misuse or wrongfully disclose it. Misuse could include the unauthorized reproduction of the personal health information.

Consent Directive – Under PHIPA, individuals may provide written instructions to health information custodians not to use or disclose their personal health information for health care purposes without their consent. Patients may essentially block all or some part of their information from one or multiple WCH agents or external health information custodians. Although the term "consent directive" is not specifically used in PHIPA, this ability to restrict use or disclosure of health information will be referred to consent directive for WCH purposes.

Disclosure – means to release or make available personal health information that is under the control or custody of a health information custodian or its authorized agent to another custodian, organization or third party outside of the circle of care.

Encryption – means using recognized techniques to transform plain electronic information into an unintelligible form that requires a special key in order to transform it back into the intelligible format.

Health Care – means any observation, examination, assessment, care, service or procedure that is done for a health-related purpose and that:

- is carried out or provided to diagnose, treat or maintain an individual's physical or mental condition, is carried out or provided to prevent disease or injury or to promote health, or is carried out or provided as part of palliative care, and includes:
    - the compounding, dispensing or selling of a drug, a device, equipment or any other item to an individual, or for the use of an individual, pursuant to a prescription, and

Health Information Custodian – means a listed person or organization under PHIPA such as hospitals, who have custody or control of personal health information as a result of the work they do. As a public hospital, WCH is considered to be a health information custodian.

Identifiable – information is identifiable if, for example, it includes the patient's name, Health File Number (HFN) or any information if either alone or with other information could be utilized to identify an individual.

Patient – means either the patient or if applicable, a person legally authorized to make decisions on the Patient's behalf (substitute decision-maker – See Appendix 1)

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

- relates to the physical or mental health of the individual, including the individual's medical history and
- the individual's family medical history;
- 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;
- relates to payment or eligibility for health care;
- is the individual's health card number; or
- identifies an individual's substitute decision-maker.

Personal Health Information Protection Act, 2004 (PHIPA) - The *Personal Health Information Protection Act, 2004* (PHIPA), is Ontario's health specific privacy legislation. PHIPA governs the manner in which personal health information may be collected, used and disclosed within the health care system. It also regulates individuals and organizations that receive personal health information from health care professionals.

Record of Personal Health Information – means personal health information in any form or in any medium whether in written, printed, photographic or electronic form or otherwise. Furthermore, any information in a health record under the custody or control of the WCH Health Information Department, any WCH clinic or service (as per the *Public Hospitals Act,* Regulation 965, Section 20), includes, but is not limited to:

- patient name,
- health file number (HFN),
- health card number,
- address,
- telephone number
- all the names of clinical staff involved in the patient's care, films, slides, diagnoses, discharge
- summaries, progress notes, transcribed reports, orders, consents, electronic images and

photographs
- any information and/or medical images in E-film or the Picture Archiving and Communication System
- (PACS)

Relative – means either of two persons who are related to each other by blood, marriage or adoption.

Research – means systematic investigation to develop or establish principles, facts or generalized knowledge or any combination of them and includes the development, testing and evaluation of research.

Researcher – means a person who conducts research.

Research Ethics Board – means a board of persons that is established for the purpose of approving research plans under PHIPA and that meets the prescribed requirements.

Security – refers to measures taken to protect personal health information against unauthorized disclosure or destruction.

Threat Risk Assessment (TRA) – is the process of assessing and mitigating threats and risks to personal health information

Use – means the handling or dealing with personal health information that is in the custody or control of WCH or its authorized agents. This includes accessing or reproducing personal health information as required by WCH.

Procedure:

1.0 Accountability for the Privacy and Confidentiality of Personal Health Information

1. WCH recognizes its obligation to respect the privacy of patients and is committed to maintaining the confidentiality of personal health information, whether written, verbal, electronic, photographic or stored on any other medium.

2. To assist with meeting our privacy obligations, WCH has a designated Privacy Office that oversees and facilitates the hospitals compliance with its privacy policies and applicable legislation.

3. It is the obligation of all of those who collect, receive and share personal health information concerning patients at WCH to exercise the utmost vigilance in the protection of patient confidentiality.

4. WCH has implemented policies and practices to give effect to this policy including:

    a. Using security safeguards to protect personal health information.
    b. Procedures to receive and respond to complaints and inquiries on privacy related matters.
    c. Signing of a Confidentiality Agreement by all agents of WCH prior to commencement of employment or affiliation with WCH.
    d. Training staff, physicians, volunteers and students and communicating to them information about PHIPA and WCH‟s policies and practices.
    e. Responding to requests for access to, or correction of, personal health information in the

custody of WCH.

f. Developing publicly available materials that explain WCH"s policies and practices.
g. Using contractual or other means to protect personal health information it discloses to third parties.

5. In compliance with PHIPA, WCH will inform patients of the loss, theft or inappropriate access of their personal health information as soon as reasonably possible.

6. Breaches of this policy and related privacy practices may be subject to disciplinary action, up to and including termination, as outlined in the Confidentiality Agreement.

7. WCH and its staff, physicians, volunteers and students (agents) are subject to the fines and penalties set out in PHIPA up to $50,000 for individuals and $250,000 for the organization.

2.0 Identifying Purposes for the Collection of Personal Health Information

1. At or before the time personal health information is collected, identify the purposes for which personal health information will be collected.

3.0 Consent for the Collection, Use & Disclosure of Personal Health Information

1. A patient who presents for treatment is considered to be giving implied consent or the use of his or her personal health information for authorized purposes.

2. The knowledgeable consent of a patient is required for the collection, use or disclosure of personal health information. The consent is knowledgeable if the patient understands the purpose of the requested collection use or disclosure and that he/she may give or withhold consent.

3. Consent does not need to be in written form; sometimes it may be implied or obtained verbally.

4. WCH may assume patient consent to collect, use and disclose his/her personal health information for the purposes of providing treatment, unless the patient tells us otherwise.

5. WCH presumes an individual is capable of consenting unless there is reason to believe otherwise.

6. If it is determined that an individual does not have capacity to consent and, in the case where the individual is a patient and has not applied for a review of your determination to the Consent and Capacity Board, the consent of the individual's substitute decision-maker should be sought. Ranking of substitute decision-makers is determined in accordance with Section 23 of the *Personal Health Information Protection Act, 2004*. (See Appendix 1)

7. In the clinical context, it is recognized that it will often be necessary to share confidential personal health information with other members of the health care team, those individuals within the patient's "circle of care".

8. Consent is not required if permitted or required by law. An example of such circumstances includes reporting a child in need of protection to a Children's Aid Society.

9. An individual may withdraw consent at any time, subject to legal restrictions and reasonable notice. For more information please see Section 7.0 Consent Directives.

4.0 Limiting Collection of Personal Health Information

1. WCH collects personal health information about patients directly from them or from the person acting on their behalf.

2. The personal health information collected may include, for example, name, date of birth, address, health history, records of visits to Women's College Hospital and the care received during those visits.

3. Occasionally, WCH collects personal health information about a patient from other sources if consent to do so has been obtained, or if the law permits.

5.0 Limiting Use and Disclosure of Personal Health Information

1. Agents of WCH have authority to access and use certain personal health information. This access is limited and strictly confined to information required for the performance of hospital duties.

2. In so far as hospital duties require, WCH agents are specifically authorized to collect and use personal health information from an individual to whom the information pertains in order to:

    a. provide health care to the individual;
    b. assist the Hospital with obtaining payment for the treatment and care (from OHIP, WSIB, a private insurer or others) provided to the individual;
    b. plan, administer and manage the Hospital and its programs;
    c. conduct risk management activities;
    d. conduct quality improvement activities (such as sending an individual a patient satisfaction survey);
    e. teach;
    f. conduct research that has been approved by the WCH Research Ethics Board or the Ethicist Assisted Process for Quality Improvements Projects (APQIP);
    g. compile statistics;
    h. comply with legal and regulatory requirements; and
    i. fulfill other purposes as permitted or required by law.

3. In the clinical context, it is recognized that it will often be necessary to share confidential personal health information with other members of the health care team, those individuals within the patient's "circle of care".

4. Information should not be shared unless there is a legitimate need to know.

5. Care should be taken to ensure that confidential information and patient records are not generally available to non-treating personnel or to others without a legitimate need to know.

6. Requests for the disclosure of personal health information should generally be referred to the Health Information Department.

7. Disclosure of personal health information is generally prohibited without the individual's consent except as outlined below:

    a. as necessary in the performance of current hospital duties.
    b. as required by statute. For example, the *Child and Family Services Act,* the *Health Protection and Promotion Act*.
    c. If the disclosure is to another health care provider and it is reasonably necessary in order to provide health care to the individual and it is not possible to obtain the individual's consent in a timely manner.
    d. When disclosing confidential personal health information will eliminate or reduce a significant risk of serious bodily harm to a patient or third parties. The first concern of the health care professional must be the safety of the patient or third party. Even when the health care professional is confronted with the necessity to disclose, confidentiality should be preserved to the maximum possible extent.
    e. In accordance with section 41 of the *Personal Health Information Protection Act* (includes court orders, summons, search warrants) or other legislation. In all instances, upon receipt of such a document, you should consult with the Risk Management Department and/or the WCH Privacy Office to ensure that the document legally authorizes the disclosure.

8. Subject to the reasonable limits described below, personal health information should never be discussed in any area where others not entitled to receive that information are present.

    For example:

    a. in public areas of the hospital such as elevators, washrooms, lounges, stairwell, or cafeteria;
    b. at home;
    c. in public places outside the hospital, unless required to do so by law or with permission from an authorized individual.

9. Because WCH is a teaching institution, opportunities may arise where the safeguarding of patient confidentiality will require extra vigilance. In the presentation of rounds, lectures or seminars, the identity of patients should not be revealed on or determinable from slides or radiological images. Under no circumstances where the instructive aspects of a clinical condition are discussed with non-WCH affiliated persons, should sufficient information be revealed to enable the identification of the patient, unless the express written consent of the patient has been obtained in advance.

10. Personal health information should not be left in written form or displayed on computer terminals in locations where it may be seen by unauthorized persons (e.g. while transporting patients and their records through the hospital or leaving information on a photocopier or fax machine).

11. Discretion should be used in determining what personal health information is placed on whiteboards that are located in patient areas. If the whiteboard is publicly accessible, the personal health information on it should, to the maximum extent possible, be limited. Medical information should not be linked to an identifiable person, especially for those patients who have asked for additional privacy protection. There may be circumstances where because of a safety concern for a patient or others, special steps may need to be taken to protect the identity of a patient. Each

situation should be considered individually and in consultation with the Risk Management and the WCH Privacy Office.

6.0 Fundraising and Marketing

1. WCH may release to WCH's Foundation the name and address only of patients, or if incapable the designated Substitute Decision Maker, for the purposes of fundraising activities for WCH.

2. A patient, or if incapable the designated Substitute Decision Maker, may request to have their name removed from WCH's fundraising contact list by contacting the WCH Foundation and/or the WCH Privacy Office.

3. WCH will not release patient contact information for marketing purposes without express consent from the patient, or if incapable Substitute Decision Maker.

7. 0 Consent Directives

1. Under the *Personal Health Information Protection Act,* patients have the right to limit or restrict how their personal health information may be used or disclosed for healthcare purposes. In some cases, a patient may not want his/her information to be used by Hospital staff or disclosed to non-WCH clinicians – such as the family doctor, or another hospital. These limitations are referred to as consent directives. For more information, please see WCH's Consent Directive Process Summary.

8.0 Media

1. All inquiries from the Media regardless of their nature should be immediately referred to the Strategic Communications Department.

2. After business hours, a Strategic Communications representative may be reached through Locating.

9.0 Telephone Inquiries

1. It is a patient's right to request that their presence at WCH not be confirmed to callers. In an ambulatory environment, staff are expected to protect patient privacy by not confirming the presence of any patient in the Hospital without the patient's express consent.

10.0 Ensuring Accuracy of Personal Health Information

1. WCH will take reasonable steps to ensure that information is as accurate, complete, and up to date as is necessary to minimize the possibility that inappropriate information may be used to make a decision about the individual.

2. Limitations on the accuracy and completeness of personal health information disclosed will be clearly set out to the recipient where possible.

11.0 Ensuring Safeguards for Personal Health Information

1. Security safeguards will be used to protect personal health information at WCH.

2. Security safeguards are used to protect personal health information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. WCH protects personal health information regardless of the format in which it is held.

3. 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.

4. The methods of protection will include:

   a. Physical measures, for example, locked filing cabinets and restricted access to offices where personal health information is held;
   b. Administrative measures (abiding by organizational policies and procedures),
   c. Technological measures (such as the use of passwords, secure computer networks, encryption and audits).

5. WCH will make its employees, physicians, volunteers and students aware of the importance of maintaining the privacy and confidentiality of personal health information. As a condition of employment, privileges or contractual arrangement at WCH, all new WCH employees/agents (e.g. employee, physician, volunteer, student, researcher, consultant, or contractor) will sign a Confidentiality Agreement with WCH. This safeguard may also be facilitated through contractual provisions.

6. Personal health information will be used only in a manner consistent with the identified purposes and will be used only by those with a need to know in fulfilling those purposes. It is prohibited to access personal health information unless required to perform duties as assigned or sanctioned by WCH. Access will only be granted to individuals for whom a signed Confidentiality Agreement is on file with WCH.

7. Anyone found accessing personal health information outside these parameters will be considered as having committed a breach of privacy and confidentiality, and will be subject to discipline, up to and including termination and/or loss of privileges.

8. Anyone granted access to personal health information by virtue of their employment or other working relationship with WCH must be prepared to present evidence of authorization to access it. Normally, for medical records, diagnostic images, etc. being requested outside the normal cycle of care and treatment, the WCH photo-identification badge and the appropriate documentation authorizing access must be presented at the time of a request to access a record. For electronic access, the unique identification and password(s) as properly issued to the requestor will normally be sufficient.

9. Any staff member asked to provide access to records has the right to request to see evidence of authorization prior to providing access, and should do so if he or she has any doubt about the authorization or identify of the requestor. If the staff member does not receive proper evidence on request, he or she has the right and obligation to refuse access.

10. Personal health information should not be discussed in any place where unauthorized persons might overhear the discussion. Even healthcare cases without patient identifiers should not be discussed, because such discussions may undermine public confidence in WCH confidentiality practice.

11. All media containing personal health information (e.g. medical records, films, ECG strips, patient wrist bands, disks, laptop computers, whiteboards, mail, drug labels, bradma cards, computer screens) must be carefully positioned, packaged, stored, transported and/or disposed of by their custodians to prevent unauthorized viewing or other access.

12. Any person observing any unattended personal health information in a public area that contains personal health information is asked to promptly forward it to and/or notify the Privacy Office, for appropriate follow-up.

13. Any portable devices (e.g. laptop, CD, USB memory key, etc) that are used to store personal health information MUST be encrypted. If there are questions or concerns regarding how to ensure devices are encrypted, staff can call the help desk for assistance, speak to their managers or contact the Privacy Office.

14. Every WCH computer user must sign a confidentiality agreement prior to being granted access to computerized personal health information. Each user is assigned a user ID and password unique to that user, which enables access to that personal health information for which access is authorized as a function of the role(s) that person performs for WCH. Authorized access is limited to the personal health information that person needs to know in order to do his or her job. Each user is responsible for maintaining the confidentiality of any assigned passwords and for ensuring no other person knows the assigned passwords.

15. Access to personal health information will be audited on a regular and consistent basis to ensure that actual access conforms to authorized access. Such audits may include review of computerized data usage by computer users, review of specific patient records for use, and review of sign-out logs for paper medical records. Inappropriate access to the system will be investigated and may result in disciplinary action up to and including termination.

16. Care will be used in the disposal or destruction of personal health information, to prevent unauthorized parties from gaining access to the information. Disposal or destruction must be in accordance with WCH policies on retention, destruction and secure disposal of personal health information. See *Secure Disposal of Personal Health Information* for more information.

12.0 Openness about Personal Health Information Policies and Practices

1. WCH makes readily available to individuals specific information about its policies and practices relating to the management of personal health information in a form that is generally understandable.

2. This includes a written public statement made available to the public. This notice:

a. provides a general description of WCH's information practices
b. describes how to contact the WCH Privacy Office (the designated privacy contact person)
b. describes how an individual may obtain access to or request correction of a record of personal health information
c. describes how an individual may make a complaint to WCH or to the Information and Privacy Commissioner of Ontario.

13.0 Individual Access to Personal Health Information

1. Individuals have the right to access personal health information maintained on them and to request amendment and correction to personal health information incorrectly recorded about them.

2. WCH also recognizes its obligation to ensure and facilitate timely access to personal health information as required by authorized individuals for direct patient care, individual administrative use, legal use, or where required to do so by law.

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

4. When an individual successfully demonstrates the inaccuracy or incompleteness of personal health information, WCH will correct the information as required. Depending upon the nature of the information challenged, correction may involve the correction, deletion, or addition of information. Where appropriate, the corrected information will be transmitted to third parties having access to the information in question.

5. When a challenge is not resolved to the satisfaction of the individual, WCH will record the substance of the unresolved challenge in the form of a written letter or statement from the patient which will be retained in the patient's medical record. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

6. A request to access a health record should be directed to the Health Information Department.

14.0 Challenging Compliance with WCH's Privacy Policies and Procedures

1. An individual will be able to address a challenge concerning privacy compliance.

2. WCH has procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal health information.

3. Complaints concerning the privacy, confidentiality and/or security of personal health information should be referred to the WCH Privacy Office, who will ensure they are properly documented and addressed.

4. All staff, physicians, volunteers and students have an obligation to ensure confidentiality of personal health information is preserved at all times.Anyone who observes a breach of confidentiality or a potential breach should enter the event into the WCH electronic incident Reporting Information System (IRIS) where it will be reviewed by the WCH Privacy Office and the WCH Quality, Risk and Safety Office

5. If appropriate, the WCH Privacy Office, will on a priority basis ensure response to the incident and will escalate the response as needed to ensure timely action.

6. Complaints and requests for information about WCH privacy policies or WCH"s compliance with them can be directed to the WCH Privacy Office at (416)323-7702 or by e-mail to privacy@wchospital.ca. In addition, or as an alternative, the requestor may be given the standard WCH brochure covering the Hospital's privacy practices.

7. Individuals may also make a complaint to the Ontario Information and Privacy Commissioner.

References:

Personal Health Information Protection Act, R.S.O. 2004, c.3. Ontario Hospital Association, (2004) Hospital

Privacy Toolkit

Canadian Standards Association Model Code for the Protection of Personal Information

Office of the Information and Privacy Commissioner

Canadian Health Information Management Association

Appendix 1

Authorized Substitute Decision Makers - Persons who may Consent on behalf of Patient
(Pursuant to Section 23 of the *Personal Health Information Protection Act, 2004)*

When a patient is not capable of providing consent to disclose their personal health information, consent may be obtained (ranked in order as listed) from the patients substitute decision maker:

1. guardian (if the guardian has the authority to make such decisions),
2. attorney for personal care or attorney for property (if the attorney has the authority to make such decisions),
3. representative (appointed by the Consent and Capacity Board under the *Health Care Consent Act, 1996* if therepresentative has the authority to give the consent),
4. spouse or partner,
5. child, custodial parent, or children's aid society or other person legally entitled to give or withhold consent in place of a parent,
6. parent with access rights,
7. brother or sister, and
8. any other relative (related by blood, marriage or adoption).

If the patient has died, consent may be obtained from the patient's estate trustee or someone who is in charge of administering the patients' estate.

To consent for a patient, the person must be:

- included in the above list,
- available and capable of consenting,
- at least 16 years old or the patients parent,
- willing to assume responsibility for giving or refusing consent,
- free of any court order or separation agreement prohibiting them from having access to or consenting for the patient, and
- the highest ranked person on the list of potential substitute decision-makers who is available and capable of consenting.

Children of any age are presumed to have the capacity to consent to the disclosure of their personal health information. Capacity should not be presumed if it is not reasonable to do so in the circumstances.

For children under 16, a parent or other lawful guardian may consent to the disclosure of personal health information even if the child has capacity, unless the information relates to:

- treatment within the meaning of the *Health Care Consent Act, 1996* about which the child has made his or her own decision, or
- Counseling in which the child has participated on his or her own under the *Child and Family Services Act*.

Consent to disclosure of personal health information about a child less than 16 years of age, may either be obtained from that child, if capable, or the parent or other lawful guardian (but not the access parent, unless such a parent has been lawfully authorized in place of the custodial parent to make information decisions). If there is a conflict between the child and the parent, the capable child's decision prevails with respect to the consent.