PRIVACY POLICY

TABLE OF CONTENTS

A. POLICY

1. It is the policy of Windsor Regional Hospital ("the Hospital") to protect the privacy and confidentiality of patient/client personal health information as required by law. This applies regardless of the format of the information. (i.e. verbal, written or electronic). The goal of these procedures is to facilitate the protection of the privacy, confidentiality, and security of patient/client personal health information held by the Hospital and to facilitate the use of that information to improve both the quality of care for patients/clients and the effective use of Hospital health care resources.

2. If a Hospital staff member has received any health care services or treatment at the Hospital, he/she is considered a patient/client in the context of this document and his/her personal health information is subject to the same policies and procedures as that of all Hospital patients/clients. Exception is provided for health care services administered under the direction of Employee Health, the documentation of which is not subject to this policy, but it shall be treated as confidential and breaches shall be subject to disciplinary action, up to and including termination of employment.

3. This policy applies to all employees and other people who work on behalf of the Hospital, including independent health care practitioners, contracted individuals, researchers, solicitors, students and volunteers.

4. This policy was developed within the context of relevant Federal and Provincial Law. Subject to a few exceptions, if there is conflict between provisions in this policy and those in another policy of the Hospital, this policy prevails unless this or the conflicting policy specifically provides otherwise. No contract or agreement that contravenes this policy may be executed or entered into by anyone to whom this policy applies.

5. Questions or complaints from the public should be directed to the Patient Relations at the applicable campus. All other inquiries regarding this policy should be directed to the Chief Privacy Officer.

6. Audits of the use of personal health information will be conducted by the Health Records Department and/or the Information Technology Department under the direction of the Chief Privacy Officer to ensure that confidentiality and privacy are maintained.

7. Violations of this policy will be reviewed and addressed.

8. All individuals shall report breaches of confidentiality of information, whether inadvertent or intentional, to their direct supervisor to ensure a prompt remedy of the occurrence (see Breach of Confidentiality). If the

breach of confidentiality is found to be serious, disciplinary action may be taken, up to and including revocation of privileges or dismissal from employment or other relationship with the Hospital.

B. PERSONAL HEALTH INFORMATION PRIVACY PRINCIPLES

This policy balances individuals' right to privacy with respect to their own personal health information with the legitimate needs of persons and organizations providing health care services to access and share this information. The Hospital has developed this policy and related procedures based on the following principles, adapted from the Canadian Standards Association's Model Code for the protection of personal information. Most privacy legislation in the world is based on these ten privacy principles. The hospital applies these principles to verbal, electronic or written personal health information used for treatment, other health care services, and research.

1. Accountability

a) Windsor Regional Hospital is responsible for personal information under our control and has designated individuals (Chief Privacy Officer and Delegates/Privacy Team) who are accountable for compliance at all hospital sites.

b) Windsor Regional Hospital complies with PHIPA by:
   i. Implementing policies and procedures to protect your personal health information, and all other confidential information including information relating to patients, staff and affiliates (Affiliates include physicians, students, volunteers, researchers, and contracted individuals who are not paid by Windsor Regional Hospital but have a working relationship with the hospital);
   ii. Responding to complaints and inquiries;
   iii. Educating our staff and affiliates about privacy policies and practices.

2. Identifying Purposes

a) Windsor Regional Hospital will identify the purposes for which personal health information is collected at or before the time of collection. These purposes will be conveyed by means of posters, brochures and the WRH web site.

b) The primary purpose to collect, use and share personal health information is to deliver patient care. We also use your information for administrative purposes, research, teaching, statistics, fundraising, and to comply with our legal and regulatory requirements.

3. Consent for the Collection, Use, and Disclosure

a) If personal health information is being used by Hospital staff to provide or assist in providing health care to registered patients/clients of the Hospital, it is reasonable to imply that the patients/clients have consented to this use. However, if a patient/client refuses to consent to a specific use, consent cannot be implied and the refusal must be respected.

b) Patients have the right to know why we are collecting their information and how it is being used.

c) Patients also have the right to withdraw their consent at any time, unless the collection, use or sharing is required or permitted by law.

4. Limiting Collection

Only the information necessary for the purposes identified may be collected. Personal health information is collected by the Hospital primarily for providing or assisting in providing health care. The purpose for which personal information is collected shall be identified by the organization at the time the information is collected.

5. Limiting Use

Personal health information may be used only for the purposes for which it was collected, except with consent or as required by law. The information is retained only as long as necessary, and securely destroyed in accordance with legislation, hospital policies, guidelines and procedures.

6. Ensuring Accuracy

Windsor Regional Hospital will make every effort to ensure the information the Hospital holds is accurate, complete and up-to-date. Patients have the right to challenge the accuracy of the information.

If a patient/client wishes to challenge the accuracy and/or completeness of the information and have it amended, they must provide a written request outlining the additional or amended information to be included as part of the permanent health record. No part of the original health record will be altered or destroyed. If the hospital disagrees with the content of the amendment, a statement of disagreement will be completed and attached to the health record. If required by the patient, the Health Records Department shall provide a copy of the statement of disagreement to any person or organization to which the health record was disclosed to in the preceding year.

7. Ensuring Safeguards

Windsor Regional Hospital applies security safeguards appropriate to the sensitivity of personal health information to aim to protect it against loss, theft, unauthorized access, disclosure, copying use, or modification, regardless of is format. Protection may include physical measures (i.e. located filing cabinets and restricted access), organizational measures (limiting access on a "need-to-know" basis), and technological measures (use of passwords, encryption and audits). New staff and affiliates are required to complete privacy

and confidentiality education and sign a confidentiality agreement as a condition of employment or affiliation. Contracted agents are bound to privacy and confidentiality as a condition of the contract.

8. Openness About Policies and Practices

Windsor Regional Hospital makes information about their privacy policies and practices available by means of posted policies and brochures at registration points and other public areas as well as on the hospital's internet site, information provided includes:

a) contact information for the hospitals' Chief Privacy Officer and /or delegate, to which complaints or inquiries can be forwarded;
b) the process for a patient to access his/her personal health information held by the hospital;
c) a description of the type of personal health information held by the hospital, including a general description of its use, and common examples of how the information may be shared.

9. Individual Access to Own Personal Information

a) Upon request, within a reasonable time and at a reasonable cost, an individual will be informed of the existence of his/her personal information and will be given access to it. They can challenge its accuracy and completeness and have it amended as appropriate.
b) Exceptions to providing access will be limited and specific. This may include information that is prohibitively costly to provide, refers to other individuals, cannot be disclosed for legal, security or proprietary reasons, and/or is subject to solicitor-client or litigation privilege.
c) An individual must provide sufficient information to permit the hospital to identify the existence of personal health information, including details of third-party recipients.

10. Challenging Compliance

An individual will be able to challenge the hospital's compliance with the hospital's policies and Privacy law to the Chief Executive Officer and/or Privacy Office delegates. Windsor Regional Hospital has procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal health information. The hospital will investigate all complaints. If a complaint is justified, Windsor Regional Hospital will take appropriate measures, including, if necessary, amending their policies and practices.

C. DEFINITIONS/KEY ABBREVIATIONS

1. Affiliate

Individuals who are not employed by WRH but perform specific tasks at or for WRH, including appointed professionals (e.g., physicians/dentists), students, volunteers, researchers, contractors, or contractor employees who may be members of a third-party contract or under direct contract to WRH and individuals working at WRH, but funded through an external source.

2. Appropriate Access

Access to health information is based on "the need to know" and circle of care guidelines (see IPC Circle of Care) to provide current and direct patient care or to perform one's duties and in alignment with established security level policies for systems. Personal health information may be used only under the following conditions:

a) **For Direct patient care** – the health care provider may access health information when they are involved in the direct and current care of the patient. Access to health information is limited to that information which is required to fulfill this purpose.
b) **Research** – personal health information may be used for this purpose once the Study is approved by the Research & Ethics Board and the designate WRH representative; however, all patient identification must be removed prior to presentation or publication of any results.
c) **Education** – personal health information may be used in education rounds for teaching purposes providing no identifiable information is disclosed. Identifiable patient information will be used only where necessary for clinical education purposes.
d) **Quality Assurance** – personal health information will be used to ensure that the quality of care and services provided to patients is of the highest quality.
e) **Patient's Personal Use** – a patient generally has a right to access his or her health information through the organizations release of information department in the health records department.
f) **As Required by Law** – personal health information may be accessed and/or released as required by law.
g) For Performance of One's Duties – personal health information may be accessed as required by individuals to perform their job duties.
h) **Other uses** – when used for purposes other than those stated here, personal information may be accessed only by persons designated by the individual or the individual legally authorized representative through a properly executed consent through the Health Records. Other uses can also include authorized access by Legal Affairs/Human Resources or designated management staff to ensure compliance with this policy and legislation.

3. Circle of Care

Is not defined in P.H.I.P.A., but refers to those in the health care team who are actually involved in the care or treatment of a particular patient.

4. Confidentiality

Means the moral, ethical, professional and employment obligation to protect the information entrusted to individuals.

5. Disclose/Disclosure

The Personal Health Information Protection Act (P.H.I.P.A.) refers to release or making available of personal health information to another person, (other than patients or their substitute decision-makers) organization or health information custodian.
It does not mean the use of the information.

6. Express /Informed Consent

Consent is informed if the patient received information about:

a) Why the information is being requested
b) The expected benefits of the release
c) The implications of the release (i.e. used against him/her)
d) Likely consequences of not releasing (i.e. warrant could be used)
e) Person received responses to his/her inquiries

Express consent can be verbal or written. If verbal, this must be documented in the chart.

7. Health Information Custodian (H.I.C.)

Defined by P.H.I.P.A. and for the purposes of WRH means any person or organization who controls other people's personal health information as part of their role as a hospital under the Public Hospitals Act, a private hospital under the Private Hospitals Act, a psychiatric facility under the Mental Health Act or an independent health facility under the Independent Health Facilities Act.

8. Health Record

Means the capture of personal health information (PHI) acquired or maintained within the organization, regardless of the medium (verbal, written, visual, electronic, microfilm/microfiche), and is the property of the H.I.C.. The PHI contained in the Health Record is owned by the patient and is considered confidential. It consists of all PHI accumulated in the following:

a) Hard-copy health records or charts housed in Health Records or designated alternative locations (e.g. Radiology)
b) Electronic patient record
c) Diagnostic images and reports, lab specimens and reports, photographs, videos, sound recordings, microfilm or microfiche
d) Departmental databases that maintain PHI

9. Implied Consent

Permits you to conclude from surrounding circumstances that a patient would reasonably agree to the collection, use or disclosure of the patient's PHI

10. Inappropriate Access

Inappropriate access occurs when an individual accesses PHI when they are not providing care for the patient and none of the appropriate access circumstances apply. Inappropriate includes, but is not limited to, accessing patient information for personal interest including one's own personal health information or that of a family member or colleague without submitting a request through the Health Records department.

11. Law Enforcement Agency

For the purpose of this policy includes Ontario Provincial Police (OPP), Royal Canadian Mounted Police (RCMP), Canadian Military Services, and municipal Police Services.

12. Most Responsible Practitioner (MRP)

For the purpose of this policy the MRP may be a physician/dentist/midwife or other Regulated Health Professional who would have knowledge of the patient and the potential risks related to disclosure of the PHI.

13. Patient Identifying Information

Means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual. Patients do not have to be named for information to be considered identifying. Information is identifying if an individual can be recognized using it, or when it can be combined with other information to identify an individual. Anonymous or de-identified personal health information cannot be linked back to the individual either directly or indirectly.

14. Patient/Substitute Decision Maker

Or **Patient/SDM** refers to the patient (if the patient is capable of making a decision with respect to the collection, use and disclosure of his or her personal health information) or the patient's Substitute Decision Maker (SDM) (if the patient is incapable with respect to the collection, use and disclosure of his or her personal health information).

15. Personal Health Information (PHI)

Defined by P.H.I.P.A. as:

Oral or recorded identifying information about someone that relates to:

a) an individual's physical or mental health, or family health history, or
b) health care an individual receives, including who provided the health care, or
c) a plan of service for an individual under the Long-Term Care Act, or
d) an individual's eligibility for health care payments or the payments made for an individual's health care, or
e) an individual's donation of any body part or bodily substance or anything derived from testing or examining a donated body part or bodily substance

Personal Health Information also includes:

f) an individual's health number
g) anything that identifies an individual's substitute decision -maker
h) anything that identifies an individual and that is contained in a personal health record

Personal health information does not include records maintained for human resources purposes.

16. Personal Information

Information about an identifiable individual, but does not include the name, title or business address or business telephone number of a staff member of an organization.

17. Quality Assurance

Refers to activities that involve the use of personal health information to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the hospital.

18. Record

Means an information record in any form or media, including written, printed, photographic or electronic format.

19. Subpoena

An Order of a Court (writ) that requires a **person** to be present at a certain time and place to testify and/or produce documents in the control of the witness or suffer a penalty. A subpoena is used to obtain testimony from a witness at both depositions (testimony under oath taken outside of court) and at trial.

20. Substitute Decision Maker (SDM)

Is defined as a person who is:

a) at least 16 years of age, unless her or she is the incapable patient's parent
b) capable with respect to the treatment
c) not prohibited by court order or separation agreement from having access to the incapable patient or giving or refusing consent on the incapable patient's behalf
d) available, and willing to assume the responsibility of giving or refusing consent

In descending order or priority, and incapable patient's SDM may be:

i. the incapable patient's "**guardian of the person**", if the guardian has authority to give or refuse consent to the treatment
ii. the incapable patient's "**attorney for personal care**", if the power of attorney confers authority to give or refuse consent to treatment
iii. the incapable patient's "**representative**" appoint by the Consent and Capacity Board, if the representative has authority to give or refuse consent to the treatment
iv. the incapable patient's **spouse** or **partner**
v. a **child or parent (custodial)** of the incapable patient, or a Children's Aid Society or other person who is lawfully entitled to give or refuse consent to the treatment in the place of the parent
vi. a **parent (who has only a right of access)** of the incapable patient
vii. a **brother or sister** of the incapable patient
viii. **any other relative** of the incapable patient.

21. Third Party Information

In relation to a patient's health record, means personal information about an identifiable individual or individuals, other than the patient.

22. Warrant

An official document, signed by a judge or other person in authority, commanding police to perform specified acts

D. CONFIDENTIAL INFORMATION

WRH has a legal and ethical responsibility to protect the privacy of patients, their families, clients and staff/hospital affiliates, and to ensure confidentiality is maintained. Confidentiality is defined as not divulging, releasing or revealing information without the express consent of the patient and/or decision maker to individuals not within the "circle of care" of the patient.

WRH considers the following types of information to be confidential:

a) Personal information and PHI regarding patients, and their families;
b) Personal information, PHI, employment information, and compensation information regarding staff and hospital affiliates; and
c) Information regarding WRH operations, which are not publicly disclosed by WRH (e.g. unpublished financial statements, legal matters, quality of care).

This policy applies whether this information is verbal, written, electronic, or in any other format.

In addition to standards of confidentiality which govern Regulated Health Professionals, staff and hospital affiliates are bound by WRH's responsibility to maintain confidentiality. WRH expects staff/hospital affiliates to keep information which they may learn or have access to because of their employment/affiliation, in the strictest confidence. It is the responsibility of every staff/hospital affiliate:

- To become familiar with and follow WRH policies and procedures regarding the use, collection, disclosure, storage, and destruction of confidential information.
- To collect, access, and use confidential information only as authorized and required to provide care of perform their assigned duties.
- To divulge, copy, transmit, or release confidential information only authorized and needed to provide care or perform their duties.
- To safeguard passwords or any other users' codes to access computer systems and programs and to assume full responsibility for activity undertaken using their security codes/passwords. This includes using access only to perform their role and not to use access on the behalf of another individual to review personal health information at the request of another party.
- To identify confidential information as such when sending e-mails or fax transmissions and to provide direction to the recipient if they receive a transmission in error.
- To discuss confidential information only with those who require this information to provide care or perform their duties and never within range (hearing or seeing) of others who should not have access to this information.
- To continue to respect and maintain the terms of the Confidentiality Agreement after an individual's employment/affiliation with the WRH ends.

1. Confidentiality Agreement

a) It is a condition of employment/privileging contract/association that staff and hospital affiliates review this policy and sign the Confidentiality Agreement before receiving access to information or records, or performing any duties at WRH (**see APPENDIX "A" – Confidentiality Agreement Form**).

b) Staff/hospital affiliates must participate in the hospital's ongoing Privacy and Confidentiality e-learning education program and any updates to the same or education provided in any format.

c) Confirmation of the successful completion of the education program and the signed confidentiality agreement will be kept on the individual's file in:
   i. Human Resources Department for staff
   ii. Volunteer Services for volunteers
   iii. Departmental Managers/Directors offices under whose supervision students, contract staff, vendors or consultants are working if not coordinated by a separate Department (i.e. any individual employed by third-party organizations who are performing work at WRH on a temporary basis)
   iv. Administration for physicians, residents, medical students, dentists, and midwives
   v. Managers must review any department specific information or procedures related to confidentiality with new staff and hospital affiliates

d) It is the responsibility of WRH to ensure that all Affiliation Agreements with education institutions include provisions outlining the obligation to ensure that students and faculty abide by the hospital's standards of confidentiality/policies and that the standard confidentiality requirements have been included in the Affiliation Agreement.

2. Breach of Confidentiality

a) A breach of confidentiality includes any inadvertent or intentional collection, use and/or disclosure of personal health information, whether verbal or written, in breach of this policy. Every person working at the Hospital has the right and responsibility to report a breach of confidentiality without fear of reprisal for doing so.

b) Staff/hospital affiliates must report suspected breaches of confidentiality, or practices within WRH that compromise confidential information, to their Departmental Manager. If the Manager is the individual suspected of the breach, staff/hospital affiliates may contact Human Resources or the Privacy Office.

c) Department Managers, in conjunction with Human Resources and/or Legal Affairs/Risk Management depending on personnel involved, will investigate alleged breaches of confidentiality. If allegations are substantiated, the individual may be subject to disciplinary action up to and including termination of employment/contract or loss of privileges or affiliation with WRH, reporting to the individual's professional College, and/or civil action/ criminal prosecution.

3. Identifying and Managing a Privacy Breach

This section provides information and direction to Supervisors/Managers when they identify or are made aware of a potential or actual privacy breach.
P.H.I.P.A. requires the organization, as a H.I.C., to take reasonable measures to protect PHI against unauthorized access, use or disclosure. Rapid action in response to an actual or potential privacy breach is part of a Supervisor's/Manager's responsibility for protecting patient's personal health information (PHI).

a) Identifying a Privacy Breach:

A privacy breach occurs whenever:

- PHI is lost or stolen, or
- PHI is accessed, disclosed, copied or modified without authority, or
- Disposal of PHI has occurred in an insecure manner, or

- In any other situation where any employee, physician, volunteer r affiliate has contravened, or is about to contravene the PHIPA.

A privacy breach can occur via verbal or written communication, by phone, e-mail, fax, electronic means or any other medium. A privacy breach can be actual, potential or suspected.

i. Privacy Breach – Actual

Includes, but is not limited to accessing patient PHI when it is not required to provide care to a patient or in the performance of work duties, for example:

- directly accessing one's own electronic health record without following the process set by Health Records
- accessing the health record of an employee, family member, friend, or any other person for whom you do not have a requirement to view information in order to provide care or perform work duties
- accessing any patient information (ex. address, date of birth, next of kin, etc.) of an employee, family member, friend, or any other person for whom you do not have a requirement to view the information in order to provide care or perform work duties

Disclosing patient information:

- without the appropriate consent, ex. to a lawyer or insurance company
- to another employee or affiliate who does not require access to the information to perform his or her job functions
- by discussing within hearing range of other people who do not require access to the information to perform his or her job functions
- by faxing or mailing to the wrong recipient in a private home or business
- by posting to a social networking site, ex. blog

Leaving patient information in unattended or unsecured locations where it may be accessed by unauthorized persons, for example:

- leaving patient reports, charts, or worksheets that contain patient-identifying information in a public area
- leaving access to electronic patient information unattended on an open log in
- storing electronic patient-identifying information on portable information devices or insecure drives, ex., hard drives that have not been encrypted
- theft of electronic devices that contain patient-identifying information
- loss of hard copy records or other patient-identifying information

ii. Privacy Breach – Potential

Occurs when an individual's PHI is at a high risk of being accessed, used or disclosed inappropriately. A potential privacy breach includes, but is not limited to situations in which:

- a patient alerts the Supervisor/Manager or the Privacy Officer that a staff member or affiliated individual may have accessed information about him or her inappropriately
- A patient requests additional security measures for his or her PHI ex. requests for anonymity and requests for patient information to be lock boxed. Contact Health Records for any request from a patient to restrict access to information.

iii. Privacy Breach – Suspected

Occurs when there has been an allegation of a privacy breach, but the allegations have not yet been substantiated or refuted by investigation.

b) Steps in the Management of a Privacy Breach

The Office of the Information and Privacy Commissioner of Ontario (I.P.C.) has directed H.I.C's to take the following steps when they identify or are made aware of a potential or actual privacy breach.

Note: Depending on the type of privacy issues, these steps may not all occur, may not be sequential and could occur concurrently.

Step 1 → Contain the breach or secure the P.H.I. to reduce the likelihood of a breach
This step may include engaging other departments, Supervisors and Managers.
Step 2 → Investigate the potential/actual breach and evaluate the risks associated with the breach
This step may include:

- Evaluating risks associated with a privacy breach.
- Creation of a privacy incident response team.
- Outcomes for employees, physicians, volunteers and affiliates.

Step 3 → Notification of those affected by the breach
This step may include:

- Notifying patients affected by the privacy breach.
- Notifying the I.P.C.

Step 4 → Managing the risk of future breaches
This step may include reducing the risk of future breaches.

Some actions are common to most privacy breach scenarios and may be referred to in each scenario. Depending on the type of breach, these actions may occur at varying steps in the investigation.

c) Criteria for Engaging Other Departments

Engaging other departments, Supervisors and Managers to assist in the management of the breach:

i. Depending on the type and severity of the breach, a Supervisor/Manager must contact the Privacy Officer as soon as reasonably possible for breaches in the "Categories of Severity for Privacy Breaches" of a rating of 2-5

ii. The Supervisor/Manager must notify the After Hours Administrator and Executive/Administrator-On-Call if:

- The breach carries a high risk, where the PHI must be immediately secured or the risk of re-occurrence is high, and/or
- The Supervisor/Manager is made aware of the breach during off-duty hours.

If the After Hours Administrator is contacted, the Supervisor/Manager must notify the Privacy Officer at the earliest reasonable time. The Privacy Officer will advise, coach and mentor the Supervisor/Manager on the need to notify or engage other Supervisors/Managers, based on the criteria for each Department:

- Risk Management
- Communications
- Human Resources
- Information Technology
- Medical Affairs
- Security
- Other personnel as necessary, depending on the breach.

d) Criteria for Notifying Risk Management of a Privacy Breach:

i. A patient or a representative of the patient indicates the intent to sue the hospital or contact a lawyer, or
ii. The information is highly sensitive and may not only identify the name of the patient, e.g. a high profile patient, but also nature of the information, or
iii. The quantity of information breached is considerable, ex., large amount of information pertaining to a single patient, or a large number of patients due to theft/loss, or
iv. External parties are investing the breach, ex., law enforcement agency, a professional College under the Regulated Health Professions Act (RHPA), the media, etc., or
v. Disciplinary action by the Hospital is a probable outcome, or
vi. Media interest is likely, e.g. the breach is a newsworthy story (see Media Requests), or
vii. A patient or employee/affiliate involved in the investigation indicates that he or she will contact the media, or
viii. An MP, MPP or a LHIN is involved or has been notified of the breach.

Severity Categories for Privacy Breaches

Notify Risk Management and Corporate Communications for Categories 3 to 5

Category	Description
1	➢ Isolated incident- non-identifiable health information ➢ Inadvertent breach using EPR(viewing of a previous screen due to incomplete system log out by user) ➢ Faxed information to wrong recipient – non-identifying, non-confidential single incident
2	➢ Faxed report to wrong recipient – PHI of a single patient
3	➢ Faxed report to wrong recipient – PHI of multiple patients ➢ Unintentional breach or release of sensitive PHI of a single patient or PHI of multiple patients due to theft or loss of files, computer or portable information storage or computer device
4	➢ Intentional unauthorized access of PHI of a single patient or multiple patients without further release to other parties
5	➢ Deliberate release of patient, employee, affiliate or organizational confidential information to the media or other parties ➢ Deliberate use or release of patient, employee, affiliate, organizational confidential information for personal gain or malice ➢ Potential for fine or penalty under the PHIPA and its regulations

e) Criteria for Notifying Corporate Communications of a Privacy Breach:

Notify Corporate Communications regarding a privacy-related incident when:

i. The incident is a level 3-5, or
ii. A law enforcement agency is a part of the investigation, or
iii. Disciplinary action by the hospital is a probable outcome, or
iv. A person involved in the investigation indicates intent to contact the media; or
v. A reporter from the media might be interested in covering the story (ex. newsworthy)

f) Criteria for Engaging Human Resources in the Management of a Privacy Breach:

i. Whenever an employee is under the investigation and/or is alleged to have breached privacy

g) Criteria for Engaging Medical Affairs in the Management of a Privacy Breach:

i. Whenever a Professional Staff member (physician, dentist) or member of SWOMEN (Southwestern Ontario Medical Education Network), medical student or privately hired physician secretary is under investigation and/or is required to speak to a Manager/Supervisor regarding a breach, or

ii. In the case of an employed physician secretary and if discipline is a probable outcome discuss with a Medical Affairs representative if Medical Affairs presence is warranted during the interview.

h) Criteria for Engaging Research Ethics Board (REB):

i. Whenever the information breached was collected and/or used for research purposes.

ii. Whenever an employee or affiliate involved in the breach was engaged in research activities.

4. Evaluating the Risks Associated with a Privacy Breach

To determine which steps are immediately necessary, it is essential to first assess the risks associated with the breach. Consider the following factors: note – the risk escalates when multiple factors are involved.

a) What kind of PHI is involved? Risk escalates if sensitive information is involved. Although all PHI is confidential and may be considered sensitive to the patient, information that may be considered more sensitive includes, but is not limited to information pertaining to:
   - Mental health
   - Sexual assault
   - Communicable diseases, ex. HIV

b) Has information been used for personal reasons or disclosed to others either in the organization or outside the organization? Disclosure increases risk. Disclosure to a non-health information custodian, ex. to a private home, business, or to an individual who is not a health care provider, carries even greater risk.

c) What is the cause of the breach? Is there a risk of an ongoing breach or further exposure?

d) Approximately how many patients are affected by the breach?

e) Are they patients of your organization? For example, if an employee or affiliated individual has accessed information inappropriately on patients who were not at your organization at the time of the access, the Privacy Officer must notify the work with the other organization to ensure compliance with our requirements under PHIPA.

f) Is the information encrypted or otherwise not easily exploited? The I.P.C. has stated: “When encryption is implemented property, it renders PHI safe from disclosure.”

g) Can the information be used for fraudulent otherwise harmful purposes?

h) What harm might the organization suffer as a result of the breach, ex. loss of trust, loss of business, loss of assets or other financial exposure?

5. Creation of a Privacy Incident Response Team

Depending on the risks associated with the breach, any of the parties involved in the breach may request that all parties meet to:

a) Facilitate the investigation
b) Identify and manage risks associated with the breach, including risk related to:
   i. reputation of the organization
   ii. patient trust
   iii. media
   iv. legal
c) Collaborate on determining next steps/actions

6. Outcomes for Employees, Affiliates, Volunteers, Physicians

Note: When referencing Employees and affiliates, volunteers and physicians are included in this group.

a) On completion of the investigation, the Manager, Supervisor, in collaboration with Human Resources, Legal or Medical Affairs (depending on which type of individual is involved) determines the most appropriate outcome for the employee or affiliate. Possible outcomes include one or more of the following:
   i. education
   ii. verbal warning
   iii. written suspension
   iv. suspension
   v. termination of relationship/placement

b) The following are examples of factors that may be considered when determining the outcome. Consult your Human Resource, Legal or Medical Affairs representative if disciplinary action is a probable outcome.
   i. Severity of the breach
   ii. Level of risk to the patient, employee and/or the organization
   iii. History of work performance or any prior discipline. Note the time lapse between disciplinary infractions and the employee's tendency to respond favorably to discipline subject to applicable collective agreement provisions
   iv. Years of service
   v. Employee or affiliate's response to and cooperation with the investigation
   vi. Whether the employee or affiliate understand the concept or privacy and confidentiality and understands the seriousness, impact and possible consequences or the breach
   vii. Provision of professional College standard

7. Notifying Patients Affected by a Privacy Breach

The Privacy Officer will advise Managers/Supervisors about the organization's legal requirement to notify:

a) A patient or incapable patient's Substitute Decision Maker (SDM), if the patient's information has been lost, stolen or accessed without authority,
b) Another organization, if the actual or potential breach involves an employee from another organization, or a patient's PHI is from another organization,

c) Other groups, based on legal, professional or contractual obligations,
d) Police, if the breach may reasonably be considered to result in significant harm to the patient or a third party,
e) The I.P.C.

8. How to Notify a Patient/SDM Affected by a Potential or Actual Privacy Breach

a) Notification of a patient/SDM may be done verbally or in writing depending on the following factors:
   i. The availability of the patient/SDM - if the patient is in hospital at the time of notification, or coming into hospital in the near future, it may be appropriate for the physician, Supervisor/Manager or the most appropriate Regulated Health Professional who has a clinical relationship with the patient, ex. Social worker, Psychologist to notify the patient in person, and
   ii. The relationship with the patient – if a physician, Supervisor/Manager, or a Regulated Health Professional has an established clinical relationship with the patient, it may be appropriate to notify the patient in person.

b) The Privacy Officer has collaborated with the IPC to develop notification letters and outlines for verbal notification and will act as a resource in the notification. The aim of notification is to be open and honest and address any questions or concerns the patient may have. Notifications should include the following information:
   i. The fact that a privacy breach occurred and a description of the breach
   ii. The elements of personal information involved, ex. exactly what information is potentially accessible to others as a result of the breach
   iii. The steps the organization has taken to mitigate the harm and reduce the risk of re-occurrence,
   iv. Advice to affected patients on what they can do to further mitigate the risk of harm, ex. to consult the Ministry of Health and Long Term Care for an audit of the use of their health card, or to obtain a new health card.

c) When responding to a patient's questions following notification of a breach, either in person, or when a patient calls in response to a notification letter, the information that may and may not be provided includes:
   i. The name of the employee/affiliate if requested by the patient
   ii. The department/area where the employee/affiliate is/was employed/affiliated
   iii. That the employee/affiliate received disciplinary action however details of the disciplinary action, ex. the specific action are not disclosed. Assure patients that the organization takes these matters very seriously and the issue has been addressed with the employee/affiliate
   iv. Details about the patient's information that was accessed (ex. In an ADT/Solcom breach) or potentially available to others (ex. laptop theft) as part of the breach. Details about how the breach occurred may be provided. For example, that the employee/affiliate searched the ADT system/Solcom by patient name and would have had access to demographic information and visit history, that the employee/affiliate opened the patient's ADT record/ Solcom, and what information that could have been accessible, ex. demographic information, laboratory and diagnostic imaging results and notes, ex. Clinic notes, discharge summaries, that were dictated using the organization's central dictation system and posted to the ADT system/Solcom.
   v. Managers/Supervisors can forward detail inquiries about access to the ADT/Solcom systems to the Privacy Officer.

d) Patients often ask if they are at risk for identity theft as a result of the breach, and whether their social insurance number was accessed. Inform the patient that we do not routinely collect SIN. The only time we collect SIN is for the first visit of a workplace injury and that we usually require a WSIB Claim # for all subsequent visits.

9. Notifying the Information and Privacy Commissioner of Ontario (IPC) The Privacy Officer will notify the IPC as needed by:

a) Preparing a de-identified summary of the issue. When applicable, the summary will indicate that the organization took disciplinary action against the employee or affiliate, without indicating the specific action. If the IPC is made aware of the specific disciplinary action, it would be required to disclose this to the patient, if requested.

b) De-identifying any written communication with the patient

c) Staff/hospital affiliates must participate annually in the hospital's Privacy and Confidentiality e-learning education program.

d) Confirmation of the successful completion of the education program and the signed confidentiality agreement will be kept on the individual's file in:
   i. Sending these document to the IPC
   ii. Liaising with the IPC for any follow up

10. Reducing the Risk of Future Breaches

Depending on the severity of the breach, any of the parties involved may initiate a review of the breach with an aim to reduce the risk of re-occurrence.

If applicable, the group may recommend steps to reduce the risk of re-occurrence. These steps may include:

a) Changes to processes, polices or procedures
b) Additional education and training for users related to PHI and their accountabilities to protect patients' privacy rights
c) Reviewing and enhancing the program or department's security measures to protect PHI

Conducting this type of review will result in continuous improvement to the PHI environment in the area and strengthen the privacy culture with the organization.

E. ACCESS TO PERSONAL HEALTH INFORMATION (PHI)

a) The record of (PHI), created, acquired or maintained, regardless of the medium (verbal, written, visual or electronic) or location for a registered patient of the organization will be under the custody and control of the HIC.
b) The Personal Information and PHI contained in the record is owned by the patient and must be kept confidential.

c) Individuals (or appropriate SDM) have a right of access to records of their own PHI except if access could result in serious harm to any person or the identification of a person who provided information in confidence.

d) All requests from a **discharged** patient/client to access his/her health record must be directed to the Health Records Department. A discharged patient/client who is mentally capable to examine his/her health record, or to consent to disclosure of his/her health record may request to examine or copy his/her health record by completing a consent to release information form and returning it to the Health Records Department.

e) If the request is for a mental health patient/client record, the Health Records Department will obtain appropriate approvals and guidelines for the access to information from the attending health care practitioner within 7 days of receipt of the request. For all current mental health patients/clients, the attending physician/health care practitioner shall be contacted for approval prior to the release for information to a patient/client. For all former mental health patients/clients, the preceding attending physician or delegate will approve the request if possible. If a decision is made to refuse the request for Mental Health records, the custodian will sever the record and provide access to the rest of the chart.

f) Direct all requests for review of an original inpatient health record by a third party, i.e. family member, lawyer, etc., to the Health Records Department. If access is approved to view the health record or part of the health record by either a discharged patient or a third party (with proper release of information), the Health Records Department or director of the patient unit will schedule an appointment for viewing. This will occur in a confidential area.

g) For **an inpatient** who requests access to his/her own chart, access to the health information will be executed in the presence of the Patient Representative, Unit Manager or designated member of the Health Records team as determined by the Director of Health Information Services.

h) Charges for copies of patient/client information will be applied as outlined in the Fee Schedule for Disclosure of Patient/Client information (Health Records Department Manual). Fees may be waived on compassionate grounds by the Manager of Health Records.

Restricted Access

i) The Hospital restricts personal access to psychiatric patient/client records according to the Mental Health Act (refer to MHA, R.S.O. 1990, Chapter M.7 (sec 35 and 36).

j) Personal information in a medical record provided by another individual (third party information) will be restricted if the third party requests in advance that the patient not be given access to the information or in a life-threatening situation. Where such a third party request is made, the third party will be advised that the Hospital will try to follow that request but may still be required by law to disclose the information

k) The Hospital will refuse an individual access to personal information if there is a significant likelihood of substantial adverse effect on the physical or mental health of the patient/client or of harm to a third party.

l) Access to a patient/client health record may be refused for reasons permitted by law which include: access is likely to result in harm to the treatment or recovery of the patient/client; or access is likely to result in injury to the mental condition of a third person, or bodily harm to a third person.

m) The Health Records Department is responsible for notifying the patient/client that his/her request has been refused.

F. DISCLOSURE OF PERSONAL HEALTH INFORMATION INCLUDING RESTRICTIONS

Disclosure of PHI must comply with legislative requirements, professional standards and the procedures outlined in this policy.
PHI may only be disclosed by the organization from which it originated, i.e. WRH must not disclose records that exist in either hard copy or electronic form that originated from a visit/admission from another organization unless under specific exceptions, and only by The Health Records Dept./DI.

1. Release of information – Health Records

a) An **Authorization to Disclosure Personal Health Information**
(Form # WRH1392) form to disclose historical information is valid for 3 months and permits the disclosure of PHI that has already been created, collected, or maintained on or before the date that the consent is signed.
The authorization for disclosure must include:

i. Name of the hospital that is to release the information
ii. Name of institution or individual that is to receive information
iii. Patient's full name and date of birth – for identification purposes
iv. Purpose or need or information, if possible
v. Specific information to be released
vi. Date form signed
   - Must be later than date of information to be released, and – cannot be more than 3 months prior to receipt of request
vii. Faxes are accepted.

No Consent is required in the following specified circumstances:

i. To contact a relative or most appropriate individual if the patient is injured, incapacitated or ill and is unable to give consent personally.
ii. Disclosures related to risks DUTY TO WARN: If the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. **Consult Legal Affairs/Risk Management/Chief Privacy Officer prior to disclosure.**
iii. Disclosures for health or other programs: Communicable Diseases to the Chief Medical Officer of Health. Consult Infectious Disease Practitioner
iv. Disclosures for proceedings: on receipt of a Warrant, Summons, or Subpoena.
v. Disclosures Complying with Mandatory Legislated Disclosure Requirements: Mandatory Gunshot Wound Reporting, Family & Children's Services Act(a child in need of protection)
vi. Disclosure for planning and management of health system, i.e. prescribed entity (CCO)
vii. For monitoring health care payments: Minister of Health
viii. Deceased patient:
   - For the purpose of identifying the individual
   - For the purpose of informing any person whom it is reasonable to inform in the circumstances of;
   - The fact the individual is deceased or suspected to be deceased
   - The circumstances of death; where appropriate
   - To the spouse, partner, sibling or child of the individual if the recipients of the information reasonably require the information to make decisions about their own health care or their children's health care (need to verify)

If unsure, contact: LEGAL AFFAIRS/RISK MANAGEMENT/PRIVACY TEAM MEMBER, HEALTH RECORDS/COORDINATOR/DIRECTOR

2. Disclosure Fees

a. A complete fee scheduled for the disclosure of documents from the hospital health record is established by and available by contacting the Health Records Dept.
b. A pre-payment of the applicable fee must accompany the consent
c. All release requests for Discharged or Deceased patients must go to Health Records

3. Research, Education and Quality Assurance

This section of the policy establishes standards for staff/affiliates regarding their access to PHI for research, education, and quality assurance purposes. This policy applies to all PHI compiled in the organization's health records, regardless of the medium or storage location.

This section does not apply to:

- The use of PHI for direct patient care, legal, or other purposes (see REFERENCES); and,
- Aggregate PHI (de-identified data) sought by staff/affiliates solely to prepare a research protocol or clinicians who wish to review their own individual patient records for the same purpose.

Only authorized staff/affiliates who have completed corporate Privacy and Confidentiality Education and signed a Privacy and Confidentiality Agreement may access PHI for research, education, and/or quality assurance purposes. Authorized staff/affiliates who access PHI for these purposes are responsible for safeguarding, disclosing, and disposing of the PHI in accordance with corporate policies on privacy, confidentiality, data security, release of information, and applicable privacy legislation.

Electronic records may only be viewed for research, education and/or quality assurance purposes in The Health Records Dept. or in other departments in which the authorized staff/affiliates have access to the

Electronic Patient Record (EPR) system /SOLCOM. There are situations where remote access can be arranged in conjunction with the Health Records Department.

Photocopies of hard-copy health records and/or the reproduction of health records in any other format must not be made without the authorization of the Manager of

Health Records (or delegate) in Health Information Management.

Regular and Ad Hoc audits are conducted to ensure compliance with this policy.

a. Education Purposes

i. Authorized staff/affiliates may access the organization's PHI for the evaluation of patient care or for internal clinical education purposes involving staff/affiliates. Identifiable patient information is used for internal teaching purposes only where necessary. PHI may be used by authorized staff/affiliates for external education purposes, provided no identifiable patient information is disclosed.
ii. Authorized staff/affiliates include members of the physician, dental and midwifery staff, allied health staff, and students assigned to the organization.
iii. Authorized staff/affiliates accessing hard-copy health records for education purposes must:
    - Submit a Request for Access to Personal Health Information for Research, Education and Quality Assurance form to the Manager or designate in Health Records;

- Present their Hospital ID badge, or other acceptable personal identification, at the time a request to review/ provide access to electronic health records for education purposes at no cost. If copies are required in unique situations, this must be reviewed with the Health Records Manager.

iv. Authorized staff/affiliates accessing the EPR (Solcom) for education purposes must document the reason for their access within each patient's EPR using the "comments" button.

b. Quality Assurance Purposes

i. With the knowledge and permission of management, staff/affiliates may access PHI to determine quality assurance or quality improvement of hospital program/services.

ii. Authorized staff/affiliates accessing hard-copy health records for quality assurance purposes must:
- Submit a Request for Access to Personal Health Information for Research, Education and Quality Assurance form to the Manager or designate in Health Records.
- Present their Hospital ID badge, or other acceptable personal identification at the time a request to review/retrieve a hard-copy health record is made.
- Health Records provides access to the health records for quality assurance purposes at not cost.

iii. Authorized staff/affiliates accessing the EPR/Solcom for quality assurance purposes must document the reason for their access within each patient's EPR using the comments section in Solcom.

c. Research Purposes

i. Staff/affiliates may access the organization's PHI for research purposes provided that:
- The research plan is approved by the Research Ethics Board and,
- A member of the research team submits a Request for Access to Personal Health Information for Research, Education and Quality Assurance form to the Manager or designate in Health Records.
- An impact analysis has been signed off and approved by the
- Health Records Manager/Director.

ii. All PHI requirements are included in the application submission process

iii. Member(s) of the research team must present their Hospital ID badge, or other acceptable personal identification, at the time a request to review/retrieve a health record is made. A Solcom workbasket is set up for the reviewer and charts put into their workbasket as required.

iv. PHI may be disclosed to a researcher only if the Research Ethics Board (R.E.B.) has approved the project or program. The R.E.B. will specify that the researcher is required to obtain written consent to the disclosure of the personal health information for the purposes of the project or program from the individuals to whom the information relates.

v. A letter of approval from the R.E.B. and any required consent forms are required for individuals wishing to use personal health information as part of any research protocol and must be presented to the Health Records Department. Depending on the nature of the request for information, a consult regarding the retrieval of the information may need to be scheduled with the Health Records Department. A list of researchers that will be accessing PHI is required and all researchers and/or assistants must sign a confidentiality agreement with hospital.

vi. When a health record is transmitted or copied for use outside the facility for the purpose of research, academic pursuits or the compilation of statistical data, the name of and any means of identifying the patient/client will be removed and a signed statement of confidentiality shall be obtained from the recipient of the information that s/he will not disclose the name of or any means of identifying the patient/client and will not use or communicate the information or material in the health record for a purpose other than research, academic pursuits or the compilation of statistical data.

4. Students

a) Students of all clinical professions, who in training at the Hospital for an official period of training, may have access to the health records on the nursing unit/program/clinic at the discretion of their supervisor and program staff.

b) For students to gain access to health records other than those located on the nursing unit/program/clinic, a written request giving the name of the patient/client and health record number, verifying the student's status and clinical involvement, signed by the student's supervisor is required. This request is to be presented to Health Records who will then authorize access to the specific record.

5. Consent and Capacity Board Hearings

a) In a proceeding before the Consent and Capacity Board, all parties shall be given an opportunity to examine and copy any documentary evidence that will be produced and any report whose contents will be given in evidence in accordance with the Health Care Consent Act (section 76(1) & (2)).

b) Upon notification of the hearing, the nursing station shall make the appropriate arrangements for the patient/client to view his/her health record if requested by the patient/client.

c) Lawyers (acting for a current inpatient) may examine the health record on the unit/program/clinic. If a lawyer requests photocopies of the health record, staff will comply with procedure for photocopying health records as outlined in this policy (see PROTECTING CONFIDENTIAL INFORMATION).

6. Rights Advisor/Lawyer

a) The Rights Advisor shall only be granted access to patient/client information, which is necessary to perform his/her routine duties (i.e. legal status, treatment status information).

b) Refer all requests for PHI from lawyers, including telephone calls, for access to health records to Health Records Department. If after hours and the request is urgent, please contact the After Hours Administrator for direction.

7. Media Requests

a) Any release of information to the media must be in compliance with the media relations practices of the Communications Department and all inquiries from the media regardless of their nature should be immediately referred to the Communications Dept.

b) After hours, the "most responsible" registered nurse, or the Supervisor and/or Admin on Call may release a one-word condition update to the media only if the reporter already has the patient's name. These updates include good, fair, serious and critical. No other information will be released without patient consent. (See Release of Information – Media Releases Policy)

8. Verbal/Telephone Requests

Basic hospital information (location and phone number) will be given out upon a request that identifies the patient/client by name as being a patient/client at the Hospital unless the patient has instructed, upon admission/registration that this information not be disclosed. In this case, the patient will be flagged in the ADT system as confidential and appear highlighted on patient census inquiry functions and documented in the patient chart indicating that no information will be released.

9. Fundraising

In general, custodians are only permitted to collect, use or disclose personal health information for non-health-care-related purposes with the express consent of the individual in question. However, provincial privacy legislation provides special rules for fundraising. It provides that a collection, use or disclosure of an individual's name and mailing address (or the name and mailing address of a substitute decision-maker, if applicable) for fundraising may take place with the implied consent of the individual in question, as long as the following requirements are met:

a) That the collection, use or disclosure of personal health information for fundraising purposes is only permitted where the fundraising relates to the charitable or philanthropic purpose related to the custodian's function;
b) That implied consent may only be inferred where the custodian has provided, or has made available, notice to the individual at the time an individual receives health care, informing that individual of the custodian's intention to use or disclose the information for fundraising purposes, along with the information on how the individual can easily opt out in your notices signs or brochures;
c) That the individual had not opted out within 60 days from the time the notice had been provided to him or her;
d) That all solicitations contain an easy opt-out from any further solicitations; and
e) That no solicitations contain information about an individual's health care or state of health.
f) Opt-out processing is coordinated by Admitting.

G. RELEASE OF INFORMATION TO LAW ENFORCEMENT AGENCIES

Section 22 of Regulation 965 under the Public Hospitals Act addresses disclosure of medical records. Except as required by law or as provided in the Act, no board shall permit any person to remove, inspect or receive information from medical records or from notes, charts and other material relating to patient care.

Where a patient has given written consent, or where a warrant is produced, information may be provided. The information provided pursuant to a warrant should be specific to what is stated in the warrant. Unless there is a clear legal duty to report, health care professionals are not required to volunteer information about patients, even to Law Enforcement Agencies.

In certain circumstances, the release of confidential information may be considered to be professional misconduct. Under the Medicine Act and Nursing Act, both provide that the giving of information concerning the condition of a patient or any services rendered to a patient, to a person other than the patient or his or her authorized representative except with the consent of the patient or his or her authorized representative or as required by law is an act of professional misconduct.

In compliance with the Public Hospitals Act and the P.H.I.P.A., law enforcement agencies require one of the following to inspect or receive information from a health record, notes, charts or other materials related to patient care, or to confiscate patient samples or patient belongings:

- Informed written consent from the patient, if capable, or the patient's Substitute Decision Maker (SDM), if the patient is incapable, or
- a warrant,

Unless the patient/SDM has placed restrictions on the disclosure of information, information that may be released without patient/SDM consent or warrant includes:

- the absence or presence of the patient in the hospital;
- a condition update of the patient (see Release of Information - Media Releases Policy)

Information may be released without patient/SDM consent:

- to a coroner or other individual (e.g. police officer) authorized by a coroner's warrant (see Coroner's Warrants and Investigations under the Coroners Act or
- to a law enforcement agent, if the patient is under arrest, or the patient is involved in a criminal investigation (these requests must be referred to the Legal Affairs/Risk Management or Admin on Call due to specific conditions on arrested patients)
- reporting treatment of a gunshot wound under the Mandatory Gunshot Wounds Reporting Act, 2005
- to a court, if staff or affiliate or the health record is **subpoenaed** (see Subpoena/Statement of Claim)

Unless there is a clear legal duty to report, staff and affiliates are not required to, and therefore should not, volunteer information about patients to law enforcement agencies.

1. Release of Information-Procedure

a) Direct law enforcement agencies that request a copy of any of the health record or department-specific records to the Health Records Dept. Health Records staff will:
   i. ensure that the appropriate documentation, i.e. consent or warrant is presented
   ii. copy/print the record/information
   iii. direct and/or facilitate requests for department-specific information to specific departments (e.g. laboratory specimens)
   iv. notify the Attending Psychiatrist when a health record contains psychiatric information. The Attending Psychiatrist then determines if there is information in the record that could be harmful to the individual or to a third party. If so determined, the Attending Psychiatrist must make a written statement to that effect for the court, by completing a Form 15-Statement by Attending Physician (available on Service Ontario website) under subsection 35(6) of the Mental Health Act.

b) The information disclosed under a warrant should include only the specific information requested in the warrant.
   i. A warrant authorizes law enforcement agencies to obtain a copy of the health record. Health Records staff must create a copy for release and keep the original paper copy for ongoing patient care.
   ii. The required form or other written consent from the patient/SDM, or warrant (or photocopy) must be placed on the hospital health record.

2. Requests to Interview Staff

a) Direct requests from law enforcement agencies to interview staff must be directed to Human Resources or after hours to the Supervisor on call. Do not disclose information about staff/affiliates (e.g. home phone or address) to law enforcement agents. The Human Resources Department can facilitate arranging an interview with staff at the organization.

b) Information, other than a "condition update" (see Release of Information – Media Interviews Policy), should not be given over the telephone to law enforcement agencies. Law enforcement agencies requesting information should make an appointment to meet with staff in person to:
   i. verify the identification of both the staff and officer
   ii. allow staff to review the health record or notes to enable them to respond appropriately

3. Subpoena/Statement of Claim

a) When a health record is subpoenaed a delegate from the Health Records Department delivers the specific health record and releases it to the presiding judge (upon his verbal/written order).

b) When a Process Server/Bailiff presents or calls to deliver a subpoena/ statement of claim:
   i. Contact the Executive Administrative Assistant to the C.E.O. (Dawn Sutherland) at 52517 if a Process Server calls or presents in the organization to deliver any legal documents (e.g. subpoena, summons to witness, statement of claim, including documents for staff members) in order that appropriate arrangements can be organized to effect service.

c) When staff receives a subpoena:
   i. Staff/affiliates do not have the authority to bring the original or a copy of the health record to court, even if it is listed in the subpoena. Staff/affiliates are only authorized to bring to court any personal notes regarding the case that they have maintained outside the Health Record.
   ii. Support for preparation for court may be facilitated through Legal Affairs/Risk Management as required.

4.Documentation of Release of Information, Patient Belongings

The Health Records Authorization for Release of Patient Information (Form), or warrant/photocopy of the warrant must be placed on the patient's health record and the following information documented on the Progress Record:

a) Summary of patient/SDM consent/refusal, if applicable,
b) Police officer's name and badge number. Ask to see photo identification to confirm,
c) Police force (e.g. OPP, Leamington Police Service) and detachment (e.g. Essex County OPP),
d) Date, time and signature of staff/affiliate releasing information, patient samples and/or belongings. The information for the physician and the person taking the samples is part of the form found in the blood kits and is given to the doctor by the investigating officer.
e) List of all documents, specimens, belongings and valuables released.

5.Coroner's Warrants and Investigations

The coroner or other individual authorized by the coroner (e.g. police officer, pathologist, and pathology assistant) may, by means of a coroner's warrant, seize information, specimens, belongings and anything else felt to be pertinent to the investigation.

a) Document receipt of a coroner's warrant and information released (see Documentation of Release of Information section) on the Clinical Progress Record of the patient's health record as outlined in the Documentation section.

b) The coroner or other individual authorized by the coroner may:
   i. ask questions of staff/affiliates for clarification
   ii. take statements from staff/affiliates
   iii. ask the identity of involved staff/affiliates
   iv. seize evidence (e.g. belongings/valuables)
   v. obtain a copy of the patient's health record

6. Reporting Gunshot Wound

It is the obligation of the organization to report to local police when a patient presents for treatment of a gunshot wound.

a) All gunshot wounds, regardless of how they occurred must be reported. This includes accidental, intentional and self-inflicted wounds, as well as those from a B.B. gun or pellet gun. The nurse in charge of the area where the patient presents (e.g. Emergency Department must report to the local police):
   i. the patient's name, if known
   ii. that the patient is being treated for a gunshot wound
   iii. the location of the facility

b) Unless the patient/SDM has placed restrictions on the disclosure of information, the nurse in charge may indicate, if asked:
   i. the disposition of the patient (e.g. admitted, discharged, and his or her location in the organization)
   ii. condition update (as in the Release of Information – Media Interviews Policy)

c) No other information can be released to police without the patient/SDM consent or warrant, including the body area affected by the gunshot and treatment to be provided.

7. Patient Lab Samples

Patient Samples:

i. Staff/affiliates may respond to inquiries from law enforcement agencies about whether blood or other samples have been taken from the patient.

ii. An informed consent from the patient/SDM or warrant is required to draw blood or take samples for purposes other than patient care/treatment.

iii. Samples and/or results are released only with an informed Health Records Authorization form from the patient/SDM, warrant or Law Enforcement agents may have a kit containing blood collection supplies and a CC 245(3) form for consent. (Samples are released only when they are no longer required to provide patient care/treatment.)

iv. The Health Records Authorization form or warrant (or photocopy) must be placed on the hospital health record.

8. Handling of Forensic Specimens

a) Any foreign object that is found in the human body should be treated as potential evidence.
b) All such objects or materials must be treated with the utmost care and attention. Minimize handling. If you must handle the specimen use a gauze square.
c) Place the specimen in a dry sterile container.
d) Any damage during handling should be noted in the health record (e.g. forceps damaging a bullet during excision in the Operating Room).
e) The specimen should be securely stored in the Unit Manager's office and released to Law Enforcement agents with the production of a warrant. Please notify Legal Affairs/ Risk Management that a forensic specimen has been removed and secured.
f) In cases where the patient is under arrest or involved in a criminal investigation, law enforcement agencies have the power to search an accused as incident to a lawful arrest and to seize anything in his/her possession or immediate surroundings to guarantee the safety of the police, members of the public in the vicinity and the accused, and to prevent the accused's escape or provide evidence against the accused. In these circumstances, it may be necessary for law enforcement agencies to be present in the OR for the removal of the foreign object.
g) Direct the Officer to the theatre and note the time of entry. Ensure awareness of sterile field. Document the Office's name and badge number on the operative record. Record specimens obtained in the usual manner. In the log book and perioperative flow sheet, note that the specimen has been given to the Officer and removed from the Hospital. Record the time the Officer leaves the OR theatre.
h) If the Officer is not present and waiting for the specimen outside the OR, record the name of the employee and time the specimen was removed from the OR. The specimen should be given directly to the authorized individual (Officer). Document accordingly in the log book and perioperative flow sheet that the specimen has been removed from the OR.

H. INFORMATION TECHNOLOGY SECURITY – GENERAL

WRH is supported by a third party Information Technology company and Regional partner, TransForm Shared Service Organization that support the operations of the hospital information technology infrastructure.

The following policy topics are addressed in TSSO policies.

1. TSSO Policies & Documentation

a) Information Security Policy
b) Information Management Policy
c) Privacy and Security Incident Management
d) Sample network Access Request Form

2. WRH Information Technology Policies

(Refer to the following WRH Policies located on the online Policy Database)

a) Appropriate Use of Email
b) Use of Personal Cell Phones and PDA's Policy
c) Network Access Codes & Mandatory Password Changes Policy
d) Remote Access to Computer Network resources Policy
e) Information Technology Usage & Standards Policy

I. PROTECTING CONFIDENTIAL INFORMATION

Every effort should be made to ensure that PHI is not inadvertently disclosed to persons who are not otherwise entitled to receive such information. Subject to the reasonable limits described below, recorded and non-recorded PHI should never be discussed, displayed or left in any area where others not entitled to do so can hear or view the information.

1. Electronic Information

a) Hospital staff are responsible for protecting PHI stored on computerized media. The Hospital retains the exclusive rights to all computer assets and information that reside on: the Hospital's mainframe processing systems, the Hospital's systems residing on local area networks, enterprise networks, and/or stand-alone microcomputers, and the Hospital's voice mail system.

b) Users should not leave a workstation unattended while a file/document containing personal health information is displayed or open, with the exception of computers in a restricted area where no unauthorized persons can view the information.

c) To secure personal health information, users must password-protect encrypted files, use screen savers and log-off when leaving a workstation unattended. Contact TSSO Service Desk, for instructions.

d) Access to computerized patient/client information will be granted in accordance with Hospital policies and procedures and access levels established. This access will be confined to information required for performance of duties.

e) E-mail and Fax Transmissions
When sending confidential information (both inside and outside WRH), e-mails and fax cover sheets must contain the following confidentiality statements:

Fax Transmissions CONFIDENTIALITY NOTICE
The contents of this telecommunication are highly confidential and intended only for the person(s) named above. Any other distribution, copying or disclosure is strictly prohibited. If you have received this telecommunication in error, please notify the sender immediately by telephone and return the original transmission to the sender by mail without making a copy.
If you do not receive all of the pages please telephone our office immediately.

E-mails CONFIDENTIALITY NOTICE
This e-mail and any files sent with it contain confidential information and are intended only for the named recipient(s). If you are not a named recipient, please telephone or e-mail the sender immediately. You should not disclose the content or take, retain, or distribute any copies.

When sending/transmitting confidential information, all WRH staff and affiliates are responsible for:

- Selecting the most secure method of sending physical (hard copy) and electronic confidential information.
- Complying with corporate faxing guidelines to reduce risk of faxing to incorrect recipients
- De-identifying, encrypting or using secure file transfer to send confidential information to a recipient outside the organization's secure network. In an e-mail that is being sent/forwarded/copied externally, the patient's/client's PHI should never appear within the e-mail. Instead, senders will use only the health record number and the patient's/client's initials.

- Not using e-mail to send confidential information to a recipient outside the hospital's secure e-mail system or ONE-Mail system.
- Designating e-mails sent within the secure e-mail system, which contain confidential information, as confidential by typing "confidential" in the subject line of the e-mail and applying the confidential status under "send options".

2. Transportation/Mail

a) If patient/client information is being physically transported/mailed within the building, it must be done in a secure manner, which ensures that PHI is not visible and that no information may be dropped or lost.
b) It is Hospital policy that no patient's original health record may be taken from the Hospital by any Hospital staff or independent health care practitioner. There are no exceptions to this policy. An active chart must be scanned in Solcom in the Health Records Dept. for cases where an urgent and immediate transfer is required. The original chart is not to leave the building.
c) If a Coroner or officer acting under the authority of the Coroner, a copy MUST be made or the chart scanned in Health Records prior to leaving the building.

3. Telephone and Cellular Telephones

Given that the cellular telephone network may not be secure, such that there is the possibility of conversations being intercepted, a regular telephone should be used whenever possible for the discussion of PHI.
If discussing PHI, the regular telephone or cellular telephone should not be used when others not entitled to hear that information are present.

4. Storage

a) PHI that is kept outside of the Health Records Dept. is subject to the same policies as if it was stored in the Health Records Dept.
b) Health records must always be stored in the Health Records Dept. unless the health record is still active and remains in use for visit. Health records must be stored in a secure area when not in use. The health record should not be left in unattended areas accessible to unauthorized individuals.

5. Photocopying

a) If any part of the legal health record or any PHI, regardless of format or storage location is photocopied in Health Records or on the unit, the same policies on confidentiality and privacy apply to the copy as if it was the original. In addition, the following information must be documented in the record: name of individual or facility to receive information; specific reports/notes photocopied; date photocopied; and, signature of individual responsible for the photocopying.
b) If the patient is still an inpatient on a patient unit and information is requested to be photocopied for continued medical care, unit clerks will make the photocopies and send/fax the copies upon validation of proper consent.
c) If the photocopies of the health record are for use outside the Hospital, Health Records staff will do the photocopying except for patient transfers.
d) If another staff member chooses to photocopy the information, he/she must ensure that a valid form for the release of information has been completed and filed.

e) Accounting staff may request copies to allow processing of health care insurance billing.

J. AUDITS

Security audits will be performed on a monthly basis and upon request to determine whether there has been a violation of privacy through inappropriate access to electronic patient information.

It is the responsibility of all users of WRH computer information systems to use electronic systems ethically, legally, and in a manner consistent with the Mission and Vision of WRH.

All individuals who have access to PHI are responsible for ensuring that the information is kept confidential and for protecting patients' privacy according to the guidelines outlined in this policy. Disciplinary action will be implemented if individuals access PHI inappropriately.

1. Regular Audits

Regular audits will be conducted and reviewed by the Privacy Team (and/or delegates) on a monthly basis on a randomly selected group of patients. This includes random accounts, random search users, random staff who are patients in the organization and others as determined by the Privacy Team.

2. Ad Hoc Audits

a) Audits can be requested by a member of the Executive or Senior Management Team, Legal Affairs/Risk Management, Human Resource Department, Physician Leader or Patient Representative on behalf of a patient (including staff who are patients), who believes patient information may have been inappropriately accessed. Please contact the Chief Privacy Officer or a member of the Privacy Team if an ad hoc report is required.

b) Audit requests and results are treated confidentially by all staff involved. The request must include the patient name, a unique identifier (MR # /Acct# if known), birth date, approximate time period of access in question or specific visit, and a brief explanation of the suspected violation including the name of the user suspected of the breach.

c) Audits are for internal purposes only. Audits may also be performed in conjunction with regional systems and auditing requirements of regionally shared systems. This includes audit processes outlined in all regional data sharing agreements. They will be conducted in a confidential manner.

K. DISPOSAL OF PHI

WRH is responsible for ensuring that all confidential information is securely maintained as required by the P.H.I.P.A.. Destruction of confidential information must be done in a manner which protects and safeguards the contents of this information and the interests of patients, employees, affiliates, and agents.

WRH uses the services of contracted third party affiliates for all of the organizations confidential waste management.

a) All information that is deemed to be confidential in nature and requires shredding will be placed in consoles marked "Shred-it" or "Iron Mountain" depending upon the site that are strategically located in departments throughout the organization.
b) The designated shredding company will be on site weekly to shred any confidential information from the consoles and provide a receipt of shredding to Environmental Services/Housekeeping. Receipts are maintained by Environmental Services/Housekeeping and coordinated with Health Records for record retention/destruction purposes.
c) When confidential consoles become too full and require emptying prior to pick up Environmental Services/Housekeeping is to be notified. The Environmental Service Department will arrange to have the console emptied and stored in a locked secured area until the shredding company makes its weekly run.
d) It is the responsibility of each department to properly identify confidential information and ensure that it is placed in the appropriate container for shredding. Departments need to be aware of appropriate legislation with respect to record retention and destruction to ensure that information being shredded meets appropriate timelines.

1. Confidential Information Requiring Shredding

a) Health Care Information
   - Patient Care Record
   - Patient-Related Administrative Information such as Schedules, Registers, Census Reports
   - Patient Blue Cards
b) Quality Assurance Information - Incident Reports, Minutes, Q.A. Reports, Evaluations, Letters
c) Business Information
   - Financial data such as pay roll - Personnel Records, Appraisals
d) Employee Health Records
e) Any Other Information Deemed Confidential - This includes all personal identifiers

2. Non-Paper Data Storage Items

a) Items include: VHS tapes, films (reel) tapes, paging system tapes, memory cards/sticks, digital camera disks, CD roms, DVD's, cassette tapes, dictation tapes, photographic images/negatives, impact printer ribbons or cartridges. Clearly label items as "Confidential".
b) Items that cannot be placed in "Shred-it" or "Iron Mountain" will be transported by Environmental Services/Housekeeping to designated locked storage room for pick up by applicable service provider.
c) After every service call a Certificate of Destruction is given to Environmental Services/Housekeeping management.
d) All confidential waste will be stored in a locked, secure area.

REFERENCES

Legislation

- Quality of Care Information Protection Act (QCIPA), 2004
- Coroners Act, R.S.O. 1990, c. C.37
- Criminal Code, R.S.C. 1985, c. C.46
- Health Care Consent Act, S.O. 1996, c. 2
- Mandatory Gunshot Wounds Reporting Act 2005, S.O. 2005, c. 9
- Mental Health Act, R.S.O. 1990, c.M.7.
- Nursing Act, 1991, S.O. 1991, c. 32
- Personal Health Information Protection Act 2004, S.O. 2004. c. 3
- Public Hospitals Act, R.S.O. 1990, c. P. 40

Other References

- London Health Sciences Centre – Release of Patient Information, Samples and/or Belongings to Law Enforcement Agencies
- HDGH Privacy Policy
- Bluewater Health Privacy Policies
- LHSC Privacy Policies
- LDMH Privacy Policies

Appendix A