Hôtel-Dieu Grace Healthcare
CHANGING LIVES TOGETHER

Title: PRIVACY	
Policy Impact: All Departments	**Document Type:** **POLICY & PROCEDURE**
Policy Owner (editor/author): Director of Risk Management & Chief Privacy Officer	**Final Approver:** Chief Financial Officer, Vice President Corporate Services & New Business Development

TABLE OF CONTENTS

POLICY

A. It is the policy of Hôtel-Dieu Grace Healthcare ("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.

B. 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 Occupational Health & Safety, 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.

C. 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.

D. 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.

E. Questions or complaints from the public should be directed to the Patient Advocate. All other inquiries regarding this policy should be directed to the Chief Privacy Officer.

F. 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.

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

H. 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.

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.

A. Accountability

1. Hôtel-Dieu Grace Healthcare is responsible for personal information under our control and has designated individuals (Chief Privacy Officer and Privacy Delegates/Privacy Team) who are accountable for compliance at all hospital sites.

2. Hôtel-Dieu Grace Healthcare complies with PHIPA by:

   a) 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 Hôtel-Dieu Grace Healthcare but have a working relationship with the hospital);

   b) responding to complaints and inquiries; and

   c) educating our staff and affiliates about privacy policies and practices.

B. Identifying Purposes

1. Hôtel-Dieu Grace Healthcare 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 HDGH website.

2. 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, quality assurance, teaching, statistics, fundraising, and to comply with our legal and regulatory requirements.

C. Consent for the Collection, Use, and Disclosure

1. 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.

2. You have the right to know why we are collecting your information and how it is being used.

3. You also have the right to withdraw your consent at any time, unless the collection, use or sharing is required or permitted by law.

D. 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.

E. Limiting Use

Personal health information may be used only for the purposes for which it was collected, except with your 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.

F. Ensuring Accuracy

Hôtel-Dieu Grace Healthcare will make every effort to ensure the information we hold 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.

G. Ensuring Safeguards

Hôtel-Dieu Grace Healthcare 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 its format. Protection may include physical measures (i.e., locked filing cabinets and restricted access), organizational measures (limiting access on a "need-to-know" basis), and technological measures (use of passwords, encryption and audits). 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.

H. Openness About Policies and Practices

Hôtel-Dieu Grace Healthcare makes information about their privacy policies and practices available by means of posted notices and brochures at registration points and other public areas as well as on the hospital's Internet site. Information provided includes:

1. contact information for the hospital's Chief Privacy Officer and/or delegate, to which complaints or inquiries can be forwarded;

2. the process for a patient to access his/her personal health information held by the hospital;

3. a description of the type of personal health information held by the hospital, including a general explanation of its use, and common examples of how the information may be shared.

I. Individual Access to Own Personal Information

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

2. 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.

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

J. 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. Hôtel-Dieu Grace Healthcare 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, Hôtel-Dieu Grace Healthcare will take appropriate measures, including, if necessary, amending their policies and practices.

DEFINITIONS

Affiliate
Individuals who are not employed by HDGH but perform specific tasks at or for HDGH, 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 HDGH and individuals working at HDGH, but funded through an external source.

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:

- **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.

- **Research** – personal health information may be used for this purpose once the study is approved by the Research & Ethics Board and the designated HDGH representative; however, all patient identification must be removed prior to presentation or publication of any results.

- **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.

- **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.

- **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.

- **As Required by Law** – personal health information may be accessed and/or released as required by law.

- **For Performance of One's Duties** – personal health information may be accessed as required by individuals to perform their job duties.

- **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's legally authorized representative through a properly executed consent through the Health information Management Department.

Circle of Care
Is not defined in the Act, but refers to those in the health care team who are actually involved in the care or treatment of a particular patient.

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

Disclose/Disclosure
The Personal Health Information Protection Act 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.

Express/Informed Consent
Consent is informed if the patient received information about:

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

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

Health Information Custodian
Means any person or organization who controls other people's personal health information as part of their role as:

- A health care practitioner or operator of a group practice of health care practitioners,
- A service provider who provides a community service under the Long-Term Care Act,
- A community care access corporation under the Community Care Access Corporations Act,
- Someone who operates one of the following facilities, programs or services;
    - 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,
    - An approved charitable home for the aged under the Charitable Institutions Act, a placement coordinator under the Charitable Institutions Act, a home or joint home under the Homes for the Aged and Rest Homes Act, a placement coordinator under the Homes for the Aged and Rest Homes Act, a nursing home under the Nursing Homes Act, a placement coordinator under the Nursing Homes Act or a care home under the Tenant Protection Act,

- A pharmacy under the Drug and Pharmacies Regulation Act,
- A laboratory or specimen collection centre under the Laboratory and Specimen Collection Centre Licensing Act,
- An ambulance service under the Ambulance Act,
- A home for special care under the Homes for Special Care Act, or
- a centre, program or service for community health or mental health whose primary purpose is to provide health care,

- an evaluator under the Health Care Consent Act or an assessor under the Substitute Decisions Act,
- a medical officer of health or a board of health under the Health Protection and Promotion Act,
- the Minister or Ministry of Health and Long-Term Care, and
- any other person described as a health information custodian under the regulations to the Act (PHIPA) with custody or control of personal health information as part of performing powers, duties or work.

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

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

PHI maintained in any other medium (i.e., microfilm/microfiche)

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 personal health information

Inappropriate Access
Inappropriate access occurs when an individual accesses personal health information 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 Information Management Department.

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.

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.

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.

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).

Personal Health Information
The Personal Health Information Protection Act, 2004 ("PHIPA") defines "Personal Health Information" as:

- Oral or recorded identifying information about someone that relates to:
    - an individual's physical or mental health, or family health history, or
    - health care an individual receives, including who provided the health care, or
    - a plan of service for an individual under the Long-Term Care Act, or
    - an individual's eligibility for health care payments or the payments made for an individual's health care, or
    - 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;
    - an individual's health number
    - anything that identifies an individual's substitute decision-maker
    - 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.

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.

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.

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

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. Lawyers use this traditional tool to ensure that witnesses present themselves at a given place, date and time to make themselves available to testify. A subpoena is used to obtain testimony from a witness at both depositions (testimony under oath taken outside of court) and at trial.

Substitute Decision-Maker (SDM)
- Is defined as a person who is:
    - at least 16 years of age, unless he or she is the incapable patient's parent
    - capable with respect to the treatment
    - 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
    - available, and willing to assume the responsibility of giving or refusing consent
- In descending order of priority, an incapable patient's SDM may be:
    - the incapable patient's **"guardian of the person"**, if the guardian has authority to give or refuse consent to the treatment;

- the incapable patient's **"attorney for personal care"**, if the power of attorney confers authority to give or refuse consent to treatment;

- the incapable patient's **"representative"** appointed by the Consent and Capacity Board, if the representative has authority to give or refuse consent to the treatment;

- the incapable patient's **spouse or partner**;

- 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;

- a **parent (who has only a right of access)** of the incapable patient;

- a **brother or sister** of the incapable patient;

- **any other relative** of the incapable patient.

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

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

CONFIDENTIAL INFORMATION

HDGH 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.

HDGH considers the following types of information to be confidential:

- Personal information and personal health information regarding patients, and their families;

- Personal information, personal health information, employment information, and compensation information regarding staff and hospital affiliates; and,

- Information regarding HDGH operations, which are not publicly disclosed by HDGH (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 HDGH's responsibility to maintain confidentiality. HDGH 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 HDGH 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 or 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.

- 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 HDGH ends.

A. Confidentiality Agreement

1. 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 HDGH (see ***APPENDIX "A"*** - Confidentiality Agreement Form).

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

3. Confirmation of the successful completion of the education program and the signed confidentiality agreement will be kept on the individual's file in:

   a) Human Resources Department for staff.

   b) Volunteer Services for volunteers.

   c) Departmental Managers/Directors offices under whose supervision students, contract staff, vendors, or consultants are working (i.e., any individual employed by third-party organizations who are performing work in the HDGH on a temporary basis).

   d) Administration for physicians, residents, medical students, dentists, and midwives.

e) Managers must review any department specific information or procedures related to confidentiality with new staff and hospital affiliates.

4. It is the responsibility of Human Resources to stipulate in Affiliation Agreements with education institutions, the obligation to ensure that students and faculty abide by the hospital's standards of confidentiality and that the standard confidentiality requirements have been included in the Affiliation Agreement.

B. Breach of Confidentiality

1. 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.

2. Staff/hospital affiliates must report suspected breaches of confidentiality, or practices within HDGH 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.

3. Department Managers, in conjunction with Human Resources, Risk Management and the Privacy Office 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 HDGH, reporting to the individual's professional College, and/or civil action/criminal prosecution.

C. 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. This guide is an inclusion to Hôtel-Dieu Grace Healthcare's Privacy Policy.

The Personal Health Information Protection Act 2004 (PHIPA) requires the organization, as a Health Information Custodian, 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).

1. 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 an employee, physician, volunteer or 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.

a) Privacy Breach – Actual

Includes, but is not limited to accessing patient personal health information 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 (i.e., 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 (i.e., 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, (i.e., 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 (i.e., 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

b) Privacy Breach – Potential

Occurs when an individual's personal health information 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 access information about him or her inappropriately
- A patient requests additional security measures for his or her personal health information (i.e., 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.

c) 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.

2. Steps in the Management of a Privacy Breach

The Office of the Information and Privacy Commissioner of Ontario has directed Health Information Custodians 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.

<u>Step 1</u> → Contain the breach or secure the Personal Health Information to reduce the likelihood of a breach.

- This step may include engaging other departments, Supervisors and Managers.

<u>Step 2</u> → 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 Information and Privacy Commissioner.

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.

3. Criteria for Engaging Other Departments

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

a) 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.

b) The Supervisor/Manager must notify the Executive/Administrator-On-Call if:

i. The breach carries a high risk, where the PHI must be immediately secured or the risk of re-occurrence is high, and/or

ii. The Supervisor/Manager is made aware of the breach during off-duty hours.

If the Executive/Administrator-On-Call is the resource 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
Information Technology	Medical Affairs
Security	Other Personnel as necessary, depending on breach

4. Criteria for Notifying Risk Management of a Privacy Breach:

a) A patient or a representative of the patient indicates the intent to sue the hospital or contact a lawyer, or

b) 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

c) 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

d) External parties are investigating the breach (i.e., law enforcement agency, a professional College under the Regulated Health Professions Act (RHPA), the media, etc.), or

e) Disciplinary action by the hospital is a probable outcome, or

f) Media interest is likely (i.e., the breach is a newsworthy story (see Media Requests), or

g) A patient or employee/affiliate involved in the investigation indicates that he or she will contact the media, or

h) 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

5. Criteria for Notifying Corporate Communications of a Privacy Breach:

Notify Corporate Communications regarding a privacy-related incident when:

a) The incident is a level 3-5, or

b) A law enforcement agency is a part of the investigation, or

c) Disciplinary action by the hospital is a probable outcome, or

d) A person involved in the investigation indicates intent to contact the media; or

e) A reporter from the media might be interested in covering the story (i.e., newsworthy)

6. Criteria for Engaging Human Resources in the Management of a Privacy Breach:

a) Whenever an employee is under investigation and/or is required to speak to a Manager/Supervisor regarding a breach, or

b) If discipline is a probable outcome, discuss with a HR representative if HR presence is needed during the interview.

7. Criteria for Engaging Medical Affairs in the Management of a Privacy Breach:

a) 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

b) 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.

8. Criteria for Engaging Research Ethics Board (REB):

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

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

D. 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.

1. 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 (i.e., HIV)
   - Genetics

2. 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 (i.e., to a private home, business, or to an individual who is not a health care provider) carries even greater risk.

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

4. Approximately how many patients are affected by the breach?

5. 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.

6. Is the information encrypted or otherwise not easily exploited? The Information and Privacy Commissioner of Ontario has stated: "When encryption is implemented properly, it renders PHI safe from disclosure."

7. Can the information be used for fraudulent or otherwise harmful purposes?

8. What harm might the organization suffer as a result of the breach (i.e., loss of trust, loss of business, loss of assets or other financial exposure?).

E. 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:

1. Facilitate the investigation

2. Identify and manage risks associated with the breach, including risk related to:

   a) reputation of the organization
   b) patient trust
   c) media
   d) legal

3. Collaborate on determining next steps/actions

F. Outcomes for Employees, Affiliates, Volunteers, Physicians

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

1. On completion of the investigation, the Manager, Supervisor, in collaboration with Human Resources 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:

   a) Education;

   b) verbal warning;

   c) written suspension;

d) suspension; and

e) termination of relationship.

2. The following are examples of factors that may be considered when determining the outcome. Consult your Human Resource/Medical Affairs representative if disciplinary action is a probable outcome.

a) Severity of the breach.

b) Level of risk to the patient, employee and/or the organization

c) 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.

d) Years of service.

e) Employee or affiliate's response to and cooperation with the investigation.

f) Whether the employee or affiliate understand the concept of privacy and confidentiality and understands the seriousness, impact and possible consequences of the breach.

G. Notifying Patients Affected by a Privacy Breach

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

1. A patient or incapable patient's Substitute Decision-Maker (SDM), if the patient's information has been lost, stolen or accessed without authority,

2. Another organization, if the actual or potential breach involves an employee from another organization, or a patient's PHI is from another organization,

3. Other groups, based on legal, professional or contractual obligations,

4. Police, if the breach may reasonably be considered to result in significant harm to the patient or a third party,

5. The Office of the Information Privacy Commissioner for Ontario (IPC)

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

1. Notification of a patient/SDM may be done verbally or in writing depending on the following factors:

a) 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 (i.e., Social worker, Psychologist) to notify the patient in person; and

b) 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.

2. 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:

a) The fact that a privacy breach occurred and a description of the breach

b) The elements of personal information involved (i.e., exactly what information is potentially accessible to others as a result of the breach),

c) The steps the organization has taken to mitigate the harm and reduce the risk of re-occurrence,

d) Advice to affected patients on what they can do to further mitigate the risk of harm (i.e., 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).

3. 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:

a) The name of the employee/affiliate if requested by the patient.

b) The department/area where the employee/affiliate is/was employed/affiliated.

c) That the employee/affiliate received disciplinary action, however details of the disciplinary action (i.e., 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

d) Details about the patient's information that was accessed (i.e., in an ADT/Solcom breach) or potentially available to others (i.e., 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.

e) Managers/Supervisors can forward detail inquiries about access to the ADT/Solcom systems to the Privacy Officer.

4. 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.

I. Notifying the Information and Privacy Commissioner of Ontario (IPC)

The Privacy Officer will notify the IPC as needed by:

1. 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.

2. De-identifying any written communication with the patient

3. Sending these document to the IPC

4. Liaising with the IPC for any follow up

J. 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:

1. Changes to processes, polices or procedures

2. Additional education and training for users related to PHI and their accountabilities to protect patients' privacy rights

3. 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

ACCESS TO PERSONAL HEALTH INFORMATION

A. The record of Personal Health Information (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 Health Information Custodian (HIC).

B. The Personal Information and Personal Health Information 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 personal health information 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 a health care practitioner and/or health record designate.

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.

Disclosure of Personal Health Information 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., HDGH 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 Department.

A. Release of Information – Health Records
(See Health Records Policy - Release of Information)

1. An **Authorization to Disclosure Personal Health Information**

(Form # 0185MI) 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:

a) name of hospital that is to release the information;

b) name of institution or individual that is to receive information;

c) patient's full name and date of birth – for identification purposes;

d) purpose or need of information, if possible;

e) specific information to be released;

f) date form signed;

   i. must be later than date of information to be released; and

   ii. cannot be more than 3 months prior to receipt of request;

g) faxes are accepted.

2. No Consent is required in the following specified circumstances:

a) To contact a relative or most appropriate individual if the patient is injured, incapacitated or ill and is unable to give consent personally.

b) 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 your Privacy Officer or Risk Manager prior to disclosure.**

c) Disclosures for health or other programs: Communicable Diseases to the Chief Medical Officer of Health. Consult Infectious Disease Practitioner.

d) Disclosures for proceedings: on receipt of a Warrant, Summons, or Subpoena.

e) Disclosures Complying with Mandatory Legislated Disclosure Requirements: Mandatory Gunshot Wound Reporting, Family & Children's Services Act (a child in need of protection).

f) Disclosure for planning and management of health system (i.e., prescribed entity [CCO]).

g) For monitoring health care payments: Minister of Health.

h) Deceased patient:

i. For the purpose of identifying the individual

ii. 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

iii. 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: PRIVACY OFFICER/RISK MANAGER, PRIVACY TEAM MEMBER, HEALTH RECORDS/COORDINATOR/DIRECTOR

B. Disclosure Fees

1. A complete fee schedule for the disclosure of documents from the hospital health record is established by and available by contacting the Health Records Dept.

2. A pre-payment of the applicable fee must accompany the consent

3. All release requests for Discharged or Deceased patients must go to Health Records.

C. 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 participated in the 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.

Audits are conducted to ensure compliance with this policy.

1. Education Purposes

a) 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.

b) Authorized staff/affiliates include members of the physician, dental and midwifery staff, allied health staff, and students assigned to the organization.

c) Authorized staff/affiliates accessing hard-copy health records for education purposes must:

i. Submit a Request for Access to Personal Health Information for Research, Education and Quality Assurance form to the Manager or designate in Health Records.

ii. 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.

d) 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.

2. Quality Assurance Purposes

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

b) Authorized staff/affiliates accessing hard-copy health records for quality assurance purposes must:

i. Submit a Request for Access to Personal Health Information for Research, Education and Quality Assurance form to the Manager or designate in Health Records.

ii. 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.

iii. Health Records provides access to the health records for quality assurance purposes at no cost.

c) 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.

3. Research Purposes

a) Staff/affiliates may access the organization's PHI for research purposes provided that:

i. The research plan is approved by the Research Ethics Board (consult with the Research Ethics Coordinator); and,

ii. 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.

iii. An impact analysis has been signed off and approved by the Health Records Manager/Director.

b) All Personal Health Information and Protection Act (PHIPA) requirements are included in the application submission process.

c) 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.

d) Personal health information 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.

e) 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.

f) 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.

D. Students

1. 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.

2. 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 the Coordinator of Health Records Department or delegate who will then authorize access to the specific record.

E. Consent and Capacity Board Hearings

1. 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)).

2. 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.

3. 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

4. **PROTECTING CONFIDENTIAL** INFORMATION).

F. Rights Advisor/Lawyer

1. 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).

2. 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 Supervisor/Admin on Call for direction.

G. Media Requests

1. Any release of information to the media must be in compliance with the Media Relations Policy. All inquiries from the media regardless of their nature should be immediately referred to the Communications Dept. The Communications Dept. can be reached Monday to Friday 9:00 a.m. to 5:00 p.m., Manager or the Admin on-call after hours or weekends.

2. 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 Media Relations Policy).

H. 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.

I. 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:

1. 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;

2. 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;

3. That the individual had not opted out within 60 days from the time the notice had been provided to him or her;

4. That all solicitations contain an easy opt-out from any further solicitations; and

5. That no solicitations contain information about an individual's health care or state of health.

6. Opt-out forms are available by contacting the Admitting Department.

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 Personal Health Information Protection Act, **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 Media Relations 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 Risk Manager or Director/Manager Health Records 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.

A. Release of Information-Procedure

1. 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:

   a) ensure that the appropriate documentation (i.e., consent or warrant is presented);

   b) copy/print the record/information;

   c) direct and/or facilitate requests for department-specific information to specific departments (i.e., laboratory specimens);

   d) 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.

2. The information disclosed under a warrant should include only the specific information requested in the warrant.

   a) 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.

b) Form # 0185 MI (Health Records Authorization for Release of Patient Information) or other written consent from the patient/SDM, or warrant (or photocopy) must be placed on the hospital health record.

B. Requests to Interview Staff

1. Direct requests from law enforcement agencies to interview staff must be directed to Human Resources or after hours to the Supervisor on-call.

2. 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.

3. Support is available from Risk Management to prepare staff and/or attend the interview with staff.

4. Information, other than a "condition update" (see Media Relations 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:

   a) verify the identification of both the staff and officer;

   b) allow staff to review the health record or notes to enable them to respond appropriately.

C. Subpoena/Statement of Claim

1. When a health record is subpoenaed the Manager of Health Records or a delegate delivers the specific health record information and releases it to the presiding judge (upon his verbal/written order).

2. When a Process Server/Bailiff presents or calls to deliver a subpoena/ statement of claim:

   a) Contact the Risk Manager if a Process Server calls or presents in the organization to deliver legal documents (e.g., subpoena, summons to witness, statement of claim).

   b) If a Process Server/Bailiff is serving a staff, contact Human Resources, they will arrange service of the documents while the staff is working in the hospital on a date, time and place that is mutually convenient to the staff and management in the area. Do not provide home contact information to a Process Server/Bailiff.

3. When staff receives a subpoena:

   a) Staff should inform Department/Program Manager and the Risk Manager of the receipt of a subpoena.

   b) The Risk Manager is available to facilitate preparation for court.

c) 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.

D. Documentation of Release of Information, Patient Belongings

The Form # 0185MI 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:

1. Summary of patient/SDM consent/refusal, if applicable;

2. Police officer's name and badge number. Ask to see photo identification to confirm;

3. Police force (i.e., OPP, Leamington Police Service) and detachment (i.e., Essex County OPP);

4. 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.

5. List of all documents, specimens, belongings and valuables released.

E. 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.

1. Document receipt of a coroner's warrant and information released (see
2.
3.
4. **Documentation of Release of Information** section) on the Clinical Progress Record of the patient's health record as outlined in the Documentation section.

5. The coroner or other individual authorized by the coroner may:

   a) ask questions of staff/affiliates for clarification

   b) take statements from staff/affiliates

   c) ask the identity of involved staff/affiliates

   d) seize evidence (e.g., belongings/valuables)

   e) obtain a copy of the patient's health record

F. Patients' Under Arrest/Investigation

1. A patient who is under arrest:

   a) A patient who is under arrest is under the authority and custody of the law enforcement agent. The agent is authorized to search a patient who is under arrest and seize his/her belongings. A warrant is required to obtain information from the chart and samples.

   b) The law enforcement agent should notify staff/affiliate that the patient is under arrest. This information and seizure of belongings must be documented in the health record.

   c) Staff and affiliates have the right to ask law enforcement agents to step outside of the room if personal care is being given to a patient. Always consider staff/affiliate safety when making these requests.

   d) The Risk Manager (or Admin on Call if not able to contact the Risk Manager) must be contacted.

2. A patient who is involved in a criminal investigation:

   a) Law enforcement agents should notify staff/affiliates that the patient is involved in a criminal investigation.

   b) This discussion must be documented in the health record.

   c) In this situation, law enforcement agents are authorized to seize the belongings of the patient that are viewable (e.g., a shirt with a bullet hole). The patient/SDM must be informed that the agent has seized the belonging.

   d) Law enforcement agents may search the patient if they believe the patient has a weapon.

3. Contact the Risk Manager and/or the Administrator-on-Call for all issues regarding the release of information, patient belongings to Law Enforcement Agencies.

INFORMATION SECURITY POLICY (APPENDIX C)

HDGH receives services from a third party Information Technology company and Regional partner (see Appendix C) that support the operations of the hospital information technology/information management infrastructure.

A. TSSO Corporate Policies & Procedure (see Appendix C)

B. HDGH Information Technology Policies

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

1. Appropriate Use of Email & Instant Messaging.

2. Corporate Mobile (Cell phone) Policy.

3. System Access Level.

4. Acceptable Use of Information Technology (IT) Resources.

5. Record Retention and Destruction.

6. Lock-Box.

PROTECTING CONFIDENTIAL INFORMATION

Every effort should be made to ensure that personal health information 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 personal health information should never be discussed, displayed or left in any area where others not entitled to do so can hear or view the information.

Examples of locations and circumstances under which this applies are:

- Public areas of the Hospital such as waiting areas, elevators, washrooms, lounges, stairwells, cafeteria or shuttle buses.
- Public places outside of the Hospital.
- Outside cover of the health record or other files.
- Photocopiers, fax machines, whiteboards that are located in patient/resident/client areas.
- Computers, personal digital assistants, etc.
- While transporting patients/clients and their records through the Hospital.

A. Electronic Information

1. Hospital staff are responsible for protecting personal health information 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.

2. 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.

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

4. 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.

5. **E-mail and Fax Transmissions: When sending confidential information (both inside and outside HDGH), emails and fax cover sheets must contain the following confidentiality statements:**

   a) **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.

   b) **Emails:**

      CONFIDENTIALITY NOTICE

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

6. When sending/transmitting confidential information, all HDGH staff and affiliates are responsible for:

a) Selecting the most secure method of sending physical (hard copy) and electronic confidential information.

b) Complying with corporate faxing guidelines to reduce risk of faxing to incorrect recipients.

c) 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.

d) Not using e-mail to send confidential information to a recipient outside the hospital's secured e-mail system or ONE-Mail system.

e) 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".

B. Transportation/Mail

1. If patient/client information is being physically transported/mailed within the building, it must be done in a secure manner, which ensures that personal health information is not visible and that no information may be dropped or lost.

2. 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.

3. 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.

C. 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 personal health information.

If a regular telephone is unavailable, refer to the Wireless Devices Policy. It should be kept to a minimum with the least possible amount of information exchanged. If discussing personal health information, the regular telephone or cellular telephone should not be used when others not entitled to hear that information are present.

D. Storage

1. Personal health information 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.

2. 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.

E. Photocopying

1. 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.

2. 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.

3. If the photocopies of the health record are for use outside the Hospital, Health Records staff will do the photocopying except for patient transfers.

4. 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.

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

F. Password Protection

1. A new password will be generated by TSSO system administrator or designated authority.

2. Do not disclose or share your password. This includes Administrative Assistants, secretaries, co-workers or family members.

3. User password management is a condition of your employment.

4. Do not write your password down. If this is unavoidable, and you need to record your password, keep it in your possession or locked at all times.

5. Do not store passwords in a file on any computer system without strong encryption.

6. Close or log out of password protected sessions when you leave your work station.

7. Passwords must be changed regularly. Frequency is set in accordance with TSSO and best practice. Old passwords should not be re-used.

8. If a password is suspected to be compromised report immediately to the Privacy Office and TSSO service desk.

9. Password format is determined in consultation with TSSO.

10. Do not use the same password for work and personal use.

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 Hôtel-Dieu Grace Hospital (HDGH) computer information systems to use electronic systems ethically, legally, and in a manner consistent with the Mission and Vision of HDGH. All staff should be familiar with the corporate policies related to Privacy and Confidentiality of Patient Information.

All individuals who have access to personal health information 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.

A. 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 and as instructed to the Application Integration Team.

B. Ad Hoc Audits

1. Audits can be requested by a member of the Senior Management Team, a Program Director, a Manager, Risk Manager, Physician Leader, Patient Representative Coordinator 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 (see Privacy Team Members) if an ad hoc report is required.

2. 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.

3. 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.

DISPOSAL OF PHI

Hôtel-Dieu Grace Healthcare (HDGH) is responsible for ensuring that all confidential information is securely maintained as required by the Personal Health Information Protection Act, 2004 (PHIPA). 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.

HDGH uses the services of a contracted third party affiliate for all of the organizations confidential waste management.

- All information that is deemed to be confidential in nature and requires shredding will be placed in consoles marked confidential that are strategically located in departments throughout the organization.

- The shredding company will be on site weekly to shred any confidential information from the consoles and provide a receipt of shredding to the Director of Environmental Services. The receipts are scanned and put in the Privacy Network Drive.

- When confidential consoles become too full and require emptying prior to pick up the Environmental Service Department 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.

- 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.

A. Confidential Information Requiring Shredding

1. Health Care Information

   a) Patient Care Record

   b) Patient-Related Administrative Information such as Schedules, Registers, Census Reports

   c) Patient Blue Cards

2. Quality Assurance Information

   a) Incident Reports, Minutes, Q.A. Reports, Evaluations, Letters

3. Business Information

   a) Financial data such as pay roll

   b) Personnel Records, Appraisals

4. Occupational Health Information

a) Employee Health Records

5. Any Other Information Deemed Confidential

a) This includes all personal identifiers

B. Paper Waste

1. Paper waste materials generated by the hospital, which contain patient information, employee information, and information related to hospital business consistent with the directives of the Privacy Office.

2. Confidential paper waste shall be placed into bags/containers dedicated specifically for that purpose. No general waste can be mixed with confidential waste. This can contaminate the confidential waste. Mixing general waste and confidential papers will result in disposing into the general waste stream. Any confidential waste not in the consoles must be tagged with a yellow confidential sticker for proper disposal.
3. Paper waste is collected and transported by "Shred-it" to a designated area for on-site shredding. Paper confidential waste is shredded on site by authorized service provider prior to leaving the premises as shredded paper.

4. All confidential paper waste should be stored in a locked, secure area.

C. Blue Identification Cards

1. Blue Patient Identification cards that are generated by the hospital upon registration and have been deemed waste.
2. Blue Patient Identification cards shall be placed into the confidential consoles dedicated and labeled specifically for that purpose.

D. Non-Paper Data Storage Items

1. All non-paper data storage waste materials generated by the Hospital which contain patient information, employee information and information related to Hospital business consistent with the directives of the Privacy Office.

   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".

2. Items that cannot be placed in "Shred-it" or confidential waste will be transported by Environmental Services to designated locked storage room for pick up by applicable service provider.

3. After every service call a Certificate of Destruction is given to the Director of Environmental Services.

4. 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

- Personal Health Information Privacy Corporate Policy - HDGH
- Media Relations Policy –HDGH
- HDH-SPD-VII Blood Alcohol Legal Format, Integrated Hospital laboratories Service
- London Health Sciences Centre – Release of Patient Information, Samples and/or Belongings to Law Enforcement Agencies
- HDGH Corporate Privacy and Confidentiality Education (e-learning)
- Bluewater Health Privacy Policies
- LHSC Privacy Policies
- LDMH Privacy Policies

Contributing Authors:

Shannon Tompkins, Director of Risk Management & Chief Privacy Officer

Alison Anderson, Director of Health Information Management, Technology & Transitions

Maureen Robbins, Coordinator of Health Records

Sheri McGeen, Director of Human Resources

APPENDIX "A"

CONFIDENTIALITY AGREEMENT

I understand that within the scope of my work and/or affiliation with Hôtel-Dieu Grace Healthcare (HDGH), I will have access to confidential information.

Definitions:

"Confidential information" means any oral, written or electronic data or information existing now or in the future relating to the operations and management of HDGH which is treated by HDGH as confidential and to which access is granted or obtained by the below name individual, and may include personal information and/or personal health information.

"Personal health information" with respect to an individual, whether living or deceased, means information concerning the physical or mental health of an individual; information concerning or collected in relation to any health service provided to the individual or information concerning the donation by any individual of any body part or bodily substance of the person. Personal health information is included in the definition of personal information.

"Personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of the organization.

1. During my work and/or affiliation with Hôtel-Dieu Grace Healthcare, I may have access to information relating to patients, medical staff, employees, volunteers and other individuals which is of a private and confidential nature. I will only access confidential information as necessary for the direct performance of my duties and responsibilities.

2. At all times, I shall respect the privacy, confidentiality and dignity of patients, employees, volunteers and all individuals associated with HDGH.

3. I shall treat all HDGH administrative, financial, patient, and employee records as confidential, and I will protect such information from improper disclosure. I shall not collect, use, alter, copy or disclose any confidential information without appropriate authorization. If I am unsure whether I have the authorization to access, use or disclose confidential information, I agree to seek clarification on this issue from my supervisor (Chief of Staff, Chief Privacy Officer, Volunteer liaison). I acknowledge that this obligation does not apply to information that is in the public domain.

4. I will be responsible for my misuse or wrongful disclosure of HDGH confidential information and for my failure to safeguard my access codes or other access authorization. I understand that my failure to comply with this Agreement may result in immediate termination of my access privileges to HDGH systems.

5. Violations of this agreement and/or HDGH policies and procedures include, but are not limited to the following examples:

- accessing confidential information that I do not require for the purpose of fulfilling my duties and responsibilities to HDGH;

- misusing, disclosing without proper authorization, or inappropriately altering personal information or personal health information;

- disclosing to another person my user name and/or password or failing to adequately protect my password.

6. I shall only access, process, and transmit confidential information using authorized hardware and software, or other authorized equipment, as required by the duties of my role at HDGH.

7. I understand that HDGH will conduct periodic audits to ensure compliance with this agreement and its privacy policy. I understand that my privileges to access confidential information are subject to periodic review, revision and discontinuance if appropriate.

8. I understand and agree to abide by the conditions outlined in this agreement, and I acknowledge that they will remain in force even after I cease to be affiliated with HDGH.

9. I also understand that, should any of these conditions be breached, I may be subject to corrective action including, but not limited to, termination of my employment or affiliation at HDGH. I also understand that there is a formal procedure for investigation of complaints and that I will have the opportunity to appeal the findings of an investigation.

10. I am aware that HDGH policies and procedures regarding privacy, confidentiality and security of personal information and I understand that it is my responsibility to be familiar with these policies and procedures and to comply with their provisions.

Name (Please Print) _____ Signature _____

Name of Witness (Please Print) _____ Signature _____

Date: _____

DISCLAIMER: When referencing any HDGH policies, users are requested to consult the online policy manual to ensure access to and use of the most current, up-to-date and accurate policy. HDGH cannot guarantee any printed policy is current or accurate, if there is a discrepancy between the electronic policy and a paper copy, the electronic copy prevails.

APPENDIX B

RISK MANAGEMENT CONTACT
(519) 257-5100 EXT. 73800
FAX (519) 257-5141
E-MAIL : stompkins@hdgh.org

HUMAN RESOURCES CONTACTS

ADMINISTRATIVE ASSISTANT:
(519) 257-5100 EXT. 73023

DIRECTOR:
(519) 257-5100 EXT . 73306
FAX (519) 257-5123

MANAGER:
(519) 257-5100 EXT. 73763

LABOUR MANAGER:
(519) 257-5100 EXT. 73874

SECURITY CONTACTS

SECURITY MANAGER:
(519) 257-5100 EXT. 73355

SECURITY OFFICE:
(519) 257-5100 EXT. 72030

COMMUNICATIONS CONTACT

COMMUNICATIONS:
(519) 257-5100 EXT. 73354

COOPERATION WITH LAW ENFORCEMENT AGENCIES

Form #
Revised April 22, 2015

INTRODUCTION

The purpose of the Co-operation with Law Enforcement Agencies (CLEA) pamphlet is:

- to minimize disruption within the hospital;
- to ensure that co-operation with law enforcement agencies is consistent; and
- to ensure the inquiry does not violate any Federal and Provincial law or infringe on a patient's rights under the Charter of Rights and Freedoms.

Any law enforcement agency requesting contact with any patient, or access to any patient information or staff member for any purpose, (i.e. delivery of subpoenas, arrest warrants, and/or collection of evidence) must direct their request through **designated** hospital personnel.

Physicians are not hospital employees and arrangements for service of subpoenas and Statements of Claim must be made with the individual physician.

DESIGNATED CONTACTS:

Monday-Friday (0800-1630 hours)

Patient Matters:
Risk Management: 257-5100 ext. 73800

Service of Subpoenas to Staff:
Human Resources: 257-5100 ext. 73023

Medical Records:
Manager: 257-5100 ext. 74104

Laboratory Matters:
Manager: 257-5100 ext. 73597

Security:
Manager: 257-5100 ext: 73355
(See back of pamphlet for alternatives)

After Hours
(Monday-Friday 1600-0800 hours, Weekends and Holidays)

Manager on Call or Admin on Call
(Contact Switchboard for on Call)

LAW ENFORCEMENT AGENCIES:

Include but are not limited to the following:

- RCMP;
- OPP;
- Local police departments;
- Provincial/Federal correctional centres;
- Department of Labour;
- Department of Immigration;
- Transport Canada; and
- Federal and Provincial Regulatory Agencies e.g. CNO, CPSO.

EXTERNAL REQUESTS FOR:

1. Law Enforcement Agency Interviews:
Requests for verbal information (interview) with ***patients***- all inquiries to be directed to Risk Management; after hours to be directed to the Manager on call; ***staff***– all inquiries to be directed to Human Resources or after hours to the Manager on call.

2. Medical Records:
Patient care record information will be released to Law Enforcement Agencies by Release of Information only if we have:

- signed authorization by the patient or his/her next-of-kin if the patient is incompetent or incapacitated; or
- a specific court order or valid search warrant.

Exception:

- By law, the Coroner is entitled to access records.

3. Photograph Requests from Law Enforcement Agencies:
All requests for photos are to be directed to Risk Management and after hours to the Director on call. Photographs may only be taken with:

- signed authorization from the patient or his/her next-of-kin if the patient is incompetent or incapacitated and only if the patient is medically able to withstand the procedure; or
- a specific court order or valid search warrant.

4. Subpoenas:
Serving of subpoenas, assistance with investigation related to staff - all inquiries to be directed to Human Resources or to the Director on call after hours. Law enforcement agencies will be highly encouraged to serve subpoenas during regular business hours (0800-1630 hours) when at all possible.

5. Search Warrants:
Search Warrants for laboratory specimens and reports are to be directed to the laboratory involved. Law enforcement agencies will be highly encouraged to serve search warrants during regular business hours (0800-1630 hours) when at all possible.

Exception:

- Coroner's Investigators do not require a Search Warrant for specimens/reports related to an investigation.

6. Visitors requiring Security Escort:
Law Enforcement Agencies providing security escort for a visitor to a patient will provide Security Services with advance notice of the visit.

7. Patients under Guard:
Law Enforcement Agencies (i.e. Correctional Services) will inform Security Services of any scheduled elective admission or outpatient diagnostic tests/ clinic visit of an individual under guard.

8. Arrest Warrants:
Warrants for the arrest of patients are to be directed to Risk Management or the Director on call, after hours.

9. Patient Condition Inquiries:
Request for updates on patient condition can be made directly to Public Affairs or the Manager on call, after hours.

APPENDIX "C"

FINAL

Manual	**CORPORATE POLICY AND PROCEDURE**		**POLICY**
Section	Information Management		
Title	**SECURITY POLICY & PROCEDURES**		
Issuing Body/ Prepared By	Zoja Holman		
Approved by	Paul Audet, Executive Lead		**Number**: 100-10
Effective Date Revised Date	August 5, 2009	Version 1	
Controlled document. Any documents appearing in paper form must be used for reference purposes only. The on-line copy on the SharePoint file server must be considered the current documentation.			

BACKGROUND

Consolidated Health Information Services (CHIS) is committed to protecting the privacy and security of the personal, personal health information (in accordance with *Personal Health Information Protection Act,* 2004, and confidential information of its clients, partners, and potential website visitors, if applicable. This policy is to ensure that personal and personal health information are safeguarded, and risk of damage to CHIS and its stakeholders are minimized.

Definition of Personal Health Information and Personal Information

I. For the purposes of this policy, *Personal health information* is any identifying information about an individual that is in verbal, written or in electronic form and relates to the following:
   - Physical or mental health, including family health history;
   - Care previously provided, including the identification of people or organization providing care;
   - Payments or eligibility for health care;
   - Donation of body parts or bodily substances (e.g. blood), or information derived from the testing of these body parts or substances;
   - An individual's health number; or
   - The name of an individual's substitute decision-maker.

- Individuals do not have to be named for information to be considered personal health information. Information is “identifying” if someone can reasonably figure out who the person might be or can deduce a person’s identity based on key pieces of information.

II. For the purposes of this policy, *Personal information* is any identifying information about an individual that is in verbal, written or in electronic form and relates to the following:
    - Bank or credit card numbers;
    - Income and payroll information (except those that meet the provincial disclosure requirements);
    - Social Insurance Numbers;
    - Home address and phone numbers;
    - Copies of resumes disclosed to the organization;
    - Performance reviews;
    - Emergency contact information; and
    - Other similar information.

POLICY

1. Overview

I. The goal of this policy is to protect the organization’s information (i.e. personal and/or personal health information) and information assets (i.e. data stored on computers, transmitted over networks, printed or written on paper, sent by fax, stored on external mobile devices, amongst others) against all internal, external, deliberate, or accidental threats.
II. The Privacy Officer has reviewed and approved this policy.
III. This policy ensures that:
    a. Information and information assets will be protected against any unauthorized access, disclosure, or disposal;
    b. Confidentiality of information will be assured;
    c. Integrity of information will be maintained;
    d. Availability of information for business processes and care processes will be maintained;
    e. Legislative and regulatory requirements (such as *Personal Health Information Protection Act,* 2004 will be met;
    f. Business continuity plans will be developed, maintained, and tested;
    g. Information security training will be available for all staff; and
    h. All actual or suspected information security incidents and breaches will be reported to the Privacy Officer and/or other appropriate oversight individuals or bodies and will be thoroughly investigated.

IV. Appropriate procedures will be developed and implemented to support this policy.
V. The Privacy Officer is responsible for maintaining and providing support and advice on this policy.

2. Security Priorities

Security at Consolidated Health Information Services (CHIS) should physically protect people (patients and staff) first, institutional information (patients and corporate) second and physical assets last. In order to attain these goals and assist with each client's mission the security should encompass technology, processes and people. If any one of those elements fails then security of assets and assurance of patient confidentiality may fail. The guiding principle will be that the level of security will be appropriate to the risk level of the asset being protected.

3. Physical Security

Physical security is CHIS's direct responsibility in conjunction additional designated Security Services departments and other departments as required to recommend physical and logical locks to maintain security at each partner organization's site.

3.1 Workstations

Publicly accessible computers will be physically secured to prevent users from removing computer workstations and associated peripherals.

3.2 Laptops

Laptops are easily stolen and should never be left unattended e.g. even a locked vehicle can be broken into. Corporate and patient data will never be stored locally on a laptop, but should be kept on servers for security and backup purposes.

3.3 Servers

In general, workgroup and Web servers will be isolated and made accessible only to system administrators and appropriate IT staff. Depending on the nature of the information stored on the servers, it may be appropriate to locate the server in a locked room or other access-controlled environment.

3.4 Network infrastructure

Routers, firewalls and other infrastructure systems will be isolated and available only to appropriate IT staff.

4. Information Security

Information security review and implementation will be the responsibility of CHIS. Assigning the value of information assets will remain with the owners of the data. Assigning levels of risk for each information asset requires input from the owners and custodians of the data.

Final decisions on acceptable levels of risk will be made by upper management (CHIS CEO and designates).

Department managers are responsible for ensuring that their staff understand and adhere to the security policy.

Tools for determining risk and protecting information assets will be provided by CHIS.

Protection of assets and information will be determined by the level of risk and value of those assets. The risks will be mitigated by technology or processes or accepted depending on senior management review. This evaluation will be based on whether the cost of a technology or process change exceeds the risk and value of an asset.

The information stored and transmitted on CHIS systems is the property of the individual managed institutions. CHIS reserves the right to monitor the use of e-mail and files as needed.

See **Acceptable Internet, Intranet and E-Mail Use 300.120** for more information on acceptable use of the systems.

4.1 Access Control

4.1.1 Identification and authentication

Users will need at least a valid user ID and password to gain access to the network or system resources. Strong, or two-factor authentication — e.g., tokens or smart cards in addition to a user ID and password — is to be used when accessing sensitive information from beyond the internal network e.g. from home or kiosks.

4.1.2 Keeping user IDs and passwords secure

User ids and passwords are to be administered by a well-defined and limited group of people. Passwords will be six to twelve characters, mixed upper and lowercase, includes numbers, doesn't have any personal information, doesn't consist of a dictionary word and isn't descriptive of work activity. Passwords will never be shared or openly published except in circumstances that severely limit access via another method e.g. publicly accessible machine with limited Internet connectivity, but no administrative rights to adjust the machine.

4.1.3 Account administration

CHIS will assign and maintain login accounts, work group privileges, e-mail addresses, any authentication devices and digital certificates across a variety of computer systems and networks. Any exceptions to the above need approval from CHIS management e.g. new accounts on PACS (Picture Archive Communication System) which may fall under the PACS administrator's responsibilities.

4.1.4 Privileged access

CHIS systems administrators will be the only users having "root," "super-user" or "admin" access to computer systems.

4.1.5 Access by non-company personnel

Contractors, patients or vendors will be allowed to access CHIS managed computer systems and network provided they have built into their contract confidentiality

clauses or alternatively have signed the **Local Guest** A**ccess – 300.55**. All external connections will be encrypted via VPN or remote access software e.g. PCAnywhere. Every effort will be made to ensure such access is for a finite period of time with appropriate expiry periods.

4.1.6 Remote access and telecommuting

Department managers will be responsible for authorizing remote access for telecommuting workers and others with a valid business need. Staff requirements for remote access will be reviewed on annually. Remote users will have to sign the **Wireless Guest Access Confidentiality Agreement** found here: **Wireless Guest Access – 300.60** All external connections will be encrypted via VPN or dialing a dedicated security server. There will be user authentication for remote access and thus an audit trail will be recorded for remote access sessions.

4.1.7 Unattended computers

When users walk away from their desks, their logged-on computer presents a network security risk. Users will lock their computers when leaving their desks. Default timeouts on HIS systems will be set to 6 minutes. Exceptions to this default will be annually reviewed. Windows and other systems timeouts will be 10 minutes.

4.1.8 Unauthorized computers

Only under strict Information Systems supervision will users be allowed to bring in and attach their own personal computers to the internal network. Such a computer will be reviewed for adequate antivirus protection and personal firewall software. Circumstances surrounding such an exception are anticipated to be vendors or external support staff requiring access. There is no expectation of IS support for such non-standard devices.

4.1.9 Electronic mail

See **Acceptable Internet, Intranet and E-Mail Use 300.120** policy for details on the use of e-mail facilities.

4.1.10 Privacy

All patient and corporate information needs to be kept private, and that employees are not permitted to access or share information that doesn't relate to their jobs. Sensitive information will be encrypted to ensure privacy while the information is in transit.

4.1.11 Message encryption

Public and Private keys will be stored in a secure location and backed up offsite. E-mail encryption tools and techniques will be defined and deployed by CHIS for secure mail exchange beyond the internal network e.g. PGP (Pretty Good Privacy).

4.1.12 Message forwarding

Caution will be exercised when forwarding e-mail messages that may contain sensitive corporate information. No patient information can be forwarded that is unsecured.

4.1.13 Message archiving

Received e-mail messages tend to accumulate and take up valuable storage space. Unfiled or deleted messages will be automatically be purged after 30 days. Exchange messages are backed up nightly, but there is still a window between receipt of a new message and immediate deletion will make the message unrecoverable.

4.2 Laptops, notebooks and handhelds

Portable computers designed for use by mobile professionals present some unique issues, and require both physical and electronic security precautions. If a portable computer is lost or stolen Information Systems and Security will be immediately notified. CHIS will disable any mobile access from the missing device and inform the Chief Privacy Officer for evaluation of any privacy breach.

4.2.1 Theft prevention

Never leave portable computers unattended. If they are exposed to the public, they will be secured both logically (with passwords) and physically (locking cable or cart).

4.2.2 Identification

Inventory control labels or other methods will be used to identify portable devices as being the property of individual institutions. The Purchasing and/or Finance departments will maintain the inventory records for portable devices. If these devices are shared by multiple people, a system of signing out and tracking who has the assets must be in place. See **Mobile Device Checkout 300.100.**

4.2.3 Mobile device access control

Desktop and portable computers require access control software forcing a user to authenticate themselves (combination of what they have and what they know e.g. users entering a user ID and password or proximity badge and password, etc.) in order to use the system. Use of a timer driven screen saver that blanks the screen and requires users to reenter credentials whenever the system has been idle for a while is highly recommended see **Unattended computers** (above). As part of the **Mobile Device Checkout** - **300.100** process security staff may need to configure each portable device's user ID, password and screen saver.

4.2.4 Preventing unauthorized observation

Users of portable devices will shield their portable devices from others when operating the equipment in public e.g. the curious eyes of airline passengers in neighboring seats will be blocked by a cardboard screening device.

4.3 File encryption

If sensitive information has to be stored on portable computers, encryption software is to be installed and used.

All Personal Health Information (PHI) transmitted or stored outside of the custodian's 'secure' corporate server or network (i.e. emailed outside of the network, remotely accessed via VPN, copied to a laptop or portable device, etc.) should be:
1) De-identified; or
2) If not able to be de-identified, should be remotely accessed via VPN; or, if not accessible via VPN,
3) encrypted.

Encryption of the PHI, while in transmission or while stored on a vulnerable computing device, is the responsibility of the disclosing custodian, unless otherwise agreed to within a data sharing agreement governing the disclosure.

4.4 Returning leased equipment

Any leased equipment that stores corporate or patient information (such as a laptop computer) will be cleared of the data before return. CHIS will have tools available to properly delete files to prevent their contents from being recovered.

4.5 Equipment repairs

Computers do fail, and sometimes need to be sent to an outside vendor for repair. Users will encrypt any sensitive files to minimize the possibly that outsiders can view proprietary information stored on “broken” computer hardware while it is being repaired or have CHIS wipe the machine to prevent the above exposure.

4.6 Disposal of removable media

Sensitive information stored on floppy disks and other removable media can be recovered even after the files have been deleted. Users will dispose of all removable media by returning the media to the local CHIS department, where it can be bulk-erased and/or physically destroyed.

5. Software security

CHIS will have access to and manage application software and its associated data, software licensing issues, computer virus prevention, and software updates and version control. External vendors may be allowed to manage specific applications under contracts agreed upon between CHIS and those organizations with appropriate confidentiality clauses in their contracts.

5.1 Access control for applications and data

Application software residing on servers will be restricted to those users whose duties require that access. The data files used by these applications will also need to be protected from unauthorized access by users not running the application.

5.2 Software license agreements

All employees will understand and adhere to the terms of software manufacturers’ license agreements because they are protected by copyright.

5.3 Personal use

Employees will not be permitted to make copies of company-purchased software for their personal use, as this typically violates software license agreements.

5.4 Installing unauthorized software

All software — commercial, public domain or shareware — will be installed by appropriate CHIS staff with appropriate management approval and will only be used for its intended purpose.

5.5 Virus control

CHIS is responsible for installing anti-virus software on corporate computer systems, and for configuring it properly and keeping its virus definition files up-to-date.

5.6 Change control.

All software upgrades must be tested for compatibility and security on non-production machines or facilities before promotion to production by CHIS or appropriately supervised vendors.

5.7 Uploading and downloading files.

All files downloaded or received as e-mail attachments need to be checked for computer viruses prior to use. Downloaded application programs, require isolated testing before widespread adoption. Users are prohibited from uploading files or attaching them to e-mail messages — software applications, proprietary source code or other intellectual property, and unencrypted sensitive corporate or patient information.

5.8 File exchange access control

Use of anonymous file transfer protocols (FTP) to exchange data and applications is restricted to non-sensitive internal company information. Use of these systems' publicly accessible directories has to be approved by management. Public information stored on these systems must be removed on a regular basis, to minimize the possibility of inappropriate information transfer. Further security measures involving stricter access control via username/password, encryption and possibly authentication devices, may be appropriate if the use of file transfer of sensitive information is being considered.

5.9 Encryption

If users are attaching sensitive information to e-mail messages, entering it into Web page forms, or uploading it to remote servers via FTP it must be encrypted appropriately to prevent it from being intercepted. The best encryption method and tools are to be applied depending on the platform being used e.g. using Secure Sockets Layer (SSL) protocols and digital certificates from an approved certificate authority and approved by CHIS.

5.10 Privacy

All users will be aware that their external electronic communications may be viewed by third parties; users will either encrypt sensitive company information, or just not send it via e-mail. See **Acceptable Internet, Intranet and E-Mail Use 300.120** policy for details on the use of e-mail facilities.

5.11 Personal Internet use

See **Acceptable Internet, Intranet and E-Mail Use 300.120**.

6. Public representation

Personal statements made public, in e-mail, newsgroups, mailing lists, bulletin boards or chat rooms, should clearly indicate that the opinions are your own (not CHIS'Ss), and must not be libelous in nature.

7. Network security

7.1 Routers and firewalls

All connections from the public Internet to internal company networks will be protected by router/firewall systems which deny services not explicitly permitted. Firewalls will be configured to only permit services which can be offered securely. For example, permit TCP/IP (Transmission Control Protocol (with Internet Protocol [IP], the main protocol of the Internet)), DNS (Domain Name System – translates names in to TCP/IP addresses), mail and news feeds from specific news servers, but block all ping queries and non-authenticated Telnet log-ins. CHIS will be responsible for maintaining and configuring CHIS'Ss network routers and firewalls and access to these functions will be severely limited.

7.2 Internet working

When connecting separate company LANs (Local Area Networks) or WANs (Wide Area Networks), we require the use of firewalls to isolate them and make their information available only to certain employees on a need-to-know basis. Also, any virtual private network (VPN) connections via the insecure public Internet will utilize encryption to insure information privacy and integrity.

7.3 Modem use

Modem access to corporate networks will only be via managed modem pools using access control and authentication. Modems should not be connected directly to users' networked computers. Remote users should not gain modem access to the network via computers that are also connected to some other network (e.g. double hop into the network).

8. Auditing and monitoring

8.1 Audit trails

An audit trail of user activity will be maintained, both at firewalls and on Web and application servers. Audit trail log files should be examined on a regular basis by security staff to determine if unauthorized activity has taken place. The retention period for the log files will be archived for a year.

8.2 Intrusion detection

Network monitoring software tools will be used to sound alarms, alerting security staff when suspicious activity occurs. Information security staff will keep these tools up to date and relevant.

8.3 Security training and awareness

Security training and awareness is important for the safety and confidentiality of patients and staff. Each employee is responsible for attending training sessions and increasing their security awareness.

9. Contingency planning

A contingency plan will be in place so everyone understands how to recover and resume normal business operations.

9.1 Backup and recovery

Mission-critical application software and data files on all computer systems should be backed up regularly, so they can be restored in case of a security disaster or system failure. Backup media should be tested periodically, and the backup data analyzed to be sure that applications and data files can be restored successfully.

9.2 Off-site storage

Copies of backup media will be periodically stored off-site far enough away to minimize the risk of damage from the same natural or man-made disaster. Off-site storage facilities will meet appropriate industry standards and should provide adequate environmental and physical protection for CHIS'Ss backup media.

10. Questions

Any questions or comments about CHIS'S information security policy and supporting procedures should be directed to the Privacy Officer.

Reference:

This policy has been developed using ISO/IEC 17799:2005[1],
The Hospital Privacy Toolkit by the Ministry of Health[2] and a Guide to Writing Security Policy[3] from the CISSP Organization's website as a basis.

Local site specific security policies may override the default policies provided here. In the absence of a local policy, these policies will provide a default security posture.

[1] http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html at April 30, 2007
[2] Hospital Privacy Toolkit, Publication #314, September 2004
[3] Guide to Writing Security Policy, RSA Inc. from CISSP Organization website http://www.cccure.org/Documents/Security_Policy/pol_guide final.pdf at April 30, 2007

DRAFT

Manual	**CHIS**		**POLICY**
Section	Information Management		
Title	**Acceptable Internet, Intranet and E-Mail Use**		
Issuing Body/ Prepared By	CHIS Policy Committee		
Approved by	CEO, Consolidated Health Information Services		**Number**: 300.120
Effective Date Revised Date	June, 2009	Version 1.0	
Controlled document. Any documents appearing in paper form must be used for reference purposes only. The on-line copy on the SharePoint file server must be considered the current documentation.			

INTERNET

POLICY

Internet access is provided to employees and officials for research or system support purposes relevant to CHIS and member organization's business and to provide such information to patients, families, interested community members, etc.

Managers and supervisors, at their discretion, may choose to block public Internet access for specific employees and/or locations.

Corporately provided Internet access and e-mail are corporate resources and are to be used for corporate business purposes.

Personal use of the Internet is authorized within reasonable limits (as determined in the sole discretion of the Corporation) as long as it does not interfere with or conflict with business use and this Policy and provided the employee has their supervisor's approval.

However, under no conditions is the Internet to be used to access sites that generally are viewed as inappropriate, for example, sites containing material which is obscene/ pornographic (including sexually explicit material, sexually explicit jokes, sexually degrading material), racially offensive/degrading, defamatory, discriminatory, hate propaganda or otherwise inappropriate.

The prime purpose of the Internet as provided to corporate employees is for corporate business.

Employees shall not knowingly:

a) Visit Internet sites that contain material which is obscene/pornographic (including sexually explicit material, sexually explicit jokes, sexually degrading material), racially offensive/degrading, defamatory, discriminatory, hate propaganda or otherwise inappropriate, without the express authorization of their supervisor for the purpose of work-related research.

b) Send or willingly receive any material which is obscene/pornographic (including sexually explicit material, full or partial nudity, sexually explicit jokes, sexually degrading material), racially offensive/degrading, defamatory, discriminatory hate propaganda or otherwise inappropriate or which is intended to annoy, harass or intimidate another person or group of persons, without the express authorization of their supervisor for the purpose of work-related research. Where an employee unwillingly receives material of this nature he or she shall report it to his or her supervisor.

c) Access, download, view, store or distribute (via email, hardcopy, images, text, video clips or otherwise) any material which is obscene/pornographic (including sexually explicit material, full or partial nudity, sexually explicit jokes, sexually degrading material), racially offensive/degrading, defamatory, discriminatory, hate propaganda, harassing or otherwise inappropriate (including jokes, images or video clips) without express authorization of their supervisor for the purposes of work-related research.

d) Revealing confidential or personal health information and any other material on chat rooms is prohibited. Personal opinions can be expressed provided a disclaimer is included that the opinion is of the individual and not the corporation as a whole. Factual information is to be expressed and distributed via the member site's Community Relations department.

e) Employees shall not, under any circumstances, use the Internet for illegal purposes, or to gather information to support illegal activities. Downloading of non-executable files for business use is permitted. These would include reports, Adobe "PDF" files, spreadsheets, information flyers, etc. Employees must ensure the source is reliable as viruses can be introduced to the system through spreadsheets and other documents. Executable software may not be downloaded without written authorization from the employee's manager. Such software, if approved, must be checked for viruses before being executed by IS. Each supervisor is responsible for their respective employees' use of the Internet. The Director, along with Human Resources, will co- ordinate any action as a result of abuse of Internet privileges.

CHIS reserves the right to restrict Internet access if use of Internet functions results in performance degradation or potential litigation against the corporation e.g. use of continuous access technology such as "Push or Pull" common to many news services, use of Instant Messaging services or access to inappropriate sites.

INTRANET

BACKGROUND
Intranet sites have been developed in order to enhance communication and improve access to information within the member organizations. Information includes member hospital and CHIS Policies and Procedures, Educational Events Calendar, library resources and much more. Data found on the site is relevant to CHIS and member sites staff, volunteers and physicians and is NOT intended for the general public. The content of the Intranet will be monitored by the Information Management Team to ensure the appropriate use of this communication tool.

POLICY
All information contained within the Intranet will be treated as as confidential to CHIS and the member organizations. Any staff, volunteer or physician who provides access to the Intranet to members of the general public will have breached confidentiality and is subject to disciplinary action.

E-MAIL

BACKGROUND
Within the CHIS and member hospital's networks, there are firewall and other monitoring devices in place that protect the security of our network. E-mail leaving our network destined to an Internet address is no longer secure. E-Mail is provided by CHIS and the member organizations to enhance professional communication and productivity. It is an integral tool used for communicating and sharing information within and across all sites within CHIS. CHIS and its member organizations own the systems and data within e-mail and are held responsible for all information transmitted on or from the system. As a result, each user should consult this policy to determine the ways in which e-mail should and should not be used.

POLICY
The CHIS e-mail system(s) are to be utilized in an appropriate, effective and efficient manner by staff and designated community partners.

General E-Mail Use
Occasional personal use is tolerated as long as it does not interfere with an employee's or physician's work, the work of others, does not generate extra costs, does not libel the organization or slander any staff member or physician and does not have a material impact on the machines' or networks' load. In no case should the e-mail be used for private business.

GUIDELINES
Each e-mail transmission creates a record that could become permanent, therefore, employees sending and/or receiving confidential or offensive material through e-mail put themselves, their jobs and the organization at risk.

1 Never email identifiable patient information to an external address.

2 Never open an attachment unless you know the sender.

3 Chain letters, jokes and inappropriate material are to be deleted permanently without being forwarded.

4 SPAM, or junk mail/advertising should be deleted permanently. Never respond to SPAM as it indicates to the sender your e-mail address is legitimate, which could lead to the receipt of more SPAM since questionable organizations could sell your address.

5 Your company e-mail address should only be given out on-line when you know the website is legitimate (e.g., registration for OHA education session, membership application/renewal, etc.).

6 Messages stored in your Inbox, Sent Box and Delete Box should be reviewed and purged regularly.

7 Employees are responsible for adhering to established security procedures, including the security of their account password, and for not bypassing security controls (i.e., disabling the anti-virus software). The employee is responsible for all use or misuse of their network and e-mail accounts.

E-mail communication shall treat individuals with respect and dignity and shall adhere to all applicable laws, regulations, and individual member institution policies. E-mail users must be aware that e-mail messages or attachments which contain offensive material or potentially offensive material (whether intentional or not) could constitute harassment. Such messages are not to be transmitted through CHIS e-mail systems.
Each CHIS employee is responsible for using electronic mail services in a manner consistent with CHIS's values. The following are examples of **inappropriate** electronic mail usage that violates our values:

- Violate intellectual property rights or laws.
- Perform illegal, unethical or immoral activities.
- Create, send or access offensive, objectionable, abusive, pornographic, sexist, racist, harassing or provocative messages, images and other materials.
- Distribute defamatory, derogatory or false messages.
- Access, without authority, other users' e-mail, data or communications.
- Infringe copyright laws.
- Disclose without authorization any member site's confidential patient, customer or employee information.
- Compromise system integrity or performance.
- Circulate personal commentary (i.e., views on government policies, political systems or political parties, religion, etc.)
- Deliberately release viruses or similar programs onto the network

Monitoring Use & Disclosure
Communication systems and data are the property of CHIS and the member organizations. CHIS reserves the right, at its sole discretion and without any further notice, to intercept, retrieve, access, review, archive, destroy, and disclose to others (including courts and law enforcement authorities), all communication systems data and uses, including e-mail. CHIS also reserves the right to limit the size of e-mail storage and transmission for all accounts. Use of the communication systems constitutes an irrevocable consent to the monitoring and disclosure of system use and data and an agreement to comply with other aspects of this policy.

Confidentiality
Users should take particular caution when circulating confidential information via e-mail. In such an example, distribution groups should be used to target the appropriate audience for confidential information. However, users should be aware that, in addition to being subject to authorized access, e-mail, in its present form, cannot be secured and is therefore vulnerable to unauthorized access and modification by third parties. Breaches can be as accidental as selecting the wrong contact in the "TO:" field or breaches can be intentional. Each user should be aware that information stored on a server or published in an e-mail could be intercepted, purposely or accidentally. A statement of confidentiality shall be appended to all internal and external e-mail.

Compliance
Inappropriate use of e-mail and therefore a breach of this policy may result in disciplinary action by CHIS up to and including termination of employment and/or affiliation with CHIS.

ACTIVE DIRECTORY USERID NAMING CONVENTION STANDARD

The following format will be used to create new user IDs (effective July 21, 2014):

hhfnnnnn where:

hh	TF – TransForm	BW – Bluewater
	CK – CKHA	HD – HDGH
	LM - Leamington	WR – Windsor Regional (Met & Ouellette)
	ST - Student	
	CC – community care (ex. CCAC, Westover)	MH – Mental Health (ex. Community ACT Team, CMHA)
	CL – Community clinics (ex. Clinics, family health)	XV – Vendor, Researchers, Consultants, Auditors
	LN – LHIN	PS – Physician Office Staff (non-Doctor)
f	The employee's first initial of the first name	
nnnnn	The employee's first five letters of the last name (can be less for short last names)	

STANDARDS:

a) AD User ID is to be all in LOWER CASE

b) Physicians will continue to use the standard established, using their CPSO ID

Physician User ID Standard:

OPTION 1 – Physicians with a 5 digit CPSO number

f	The Physician's first name initial
n	The Physician's last name initial
0	Zero
12345	The Physician's 5 digit CPSO number

OPTION 2 – Physicians with a 6 digit CPSO number

f	The Physician's first name initial
n	The Physician's last name initial
123456	The Physician's 6 digit CPSO number

If a duplicate is encountered, the format below will be used for the specific user ID.

hhff(c)nnnn where:

hh	TF – TransForm	BW – Bluewater
	CK – CKHA	HD – HDGH
	LM - Leamington	WR – Windsor Regional (Met & Ouellette)
	ST - Student	
	CC – community care (ex. CCAC, Westover)	MH – Mental Health (ex. Community ACT Team, CMHA)
	CL – Community clinics (ex. Clinics, family health)	XV – Vendor, Researchers, Consultants, Auditors
	LN – LHIN	PS – Physician Office Staff (non-Doctor)
f	The employee's first initial of the first name	
f(c)	The employee's first name – first consonant (ie Kathy would be "kt")	
nnnn	The employee's first four letters of the last name (can be less for short last names)	

If a duplicate is still encountered, the format below will be used for the specific user ID.

hhff(c)f(c)nnn where:

hh	TF – TransForm	BW – Bluewater
	CK – CKHA	HD – HDGH
	LM - Leamington	WR – Windsor Regional (Met & Ouellette)
	ST - Student	
	CC – community care (ex. CCAC, Westover)	MH – Mental Health (ex. Community ACT Team, CMHA)
	CL – Community clinics (ex. Clinics, family health)	XV – Vendor, Researchers, Consultants, Auditors
	LN – LHIN	PS – Physician Office Staff (non-Doctor)
f	The employee's first initial of the first name	
f(c)	The employee's first name – first consonant (ie Kathy would be "kt")	
f(c)	The employee's first name – second consonant (ie Kathy would be "kth")	
nnn	The employee's first three letters of the last name (can be less for short last names)	

Any duplicates not covered by any of the three formats above will be dealt with as required.

REQUESTING NAME CHANGES STANDARD

The following standard exists as it relates to requests to change the user id:

Date	Explanation
09-30-2014	It is the Hospital's policies not to change user ids (ex. due to marriage, divorce, etc)

APPLICATION USERID NAMING CONVENTION STANDARD

Application IDs will follow the AD standard, knowing there may be some variations, due to application specifics.

PASSWORD CONVENTION STANDARD

Standardizing on initial passwords and password resets:

Date	Explanation
09-30-2014	Initial passwords for WRM and WRO should be set to “changeme”. Only for non-application passwords to start.