Security & Confidentiality of Personal & Personal Health Info			
Identifier:		Version #:	1.4
Folder:	PRIVACY	Type:	POLICY - 2 YEAR
Subfolder:	POLICIES & PROC	Effective on:	26-07-2018

Preamble:
Individuals have an ethical and legal right to privacy. The Geraldton District Hospital (GDH) recognizes its obligation to respect privacy and is committed to maintaining the confidentiality of patient, employee, and corporate information, whether written, verbal, electronic, photographic or stored on any other medium. The Geraldton District Hospital has developed and implemented security safeguards to protect personal information and personal health information against loss, theft, unauthorized access, disclosure, copying, use or modification.

POLICY:
Personal information and personal health information shall be protected by security safeguards appropriate to the sensitivity of the information. Care will be used in the disposal or destruction of information, to prevent unauthorized parties from gaining access to the information. This policy applies to all Hospital employees and its affiliates (physicians, volunteers, students, etc.).

What is confidential information?
Confidential information is information of a sensitive nature in any format, which is created or received by the Hospital in the course of its business, which is not otherwise available to the public and includes, but is not limited, to the following:

Patient Information:
Any information that could lead to the identification of a specific patient, or family member/significant other of the patient, health records, conversations/discussions regarding condition or treatment, financial/family circumstances.

Financial Information:
Any information in relation to an individual's salary or any unpublished financial information (i.e.: payroll).

Human Resources Information:
Performance-related information, compensation, benefits, occupational health information, family/personal circumstances.

Legal Information:
Any information related to a legal document (disputes, contracts).

Human Rights Information:
Information associated with an informal or formal human rights complaint, including abuse, harassment complaint.

Other Administrative Information:
Any information used for administrative purposes (i.e. patient census, employee lists, patient lists).

Hospital Business:
Financial/statistical information, strategic planning initiatives i.e. organization restructuring, merging, outsourcing.

The methods of protection include physical, administrative and technical measures.

- Individuals will access confidential information only to the extent necessary to perform current hospital duties, on a **"need-to-know"** basis. Except as required in the performance of a task related to a specific patient or work assignment within the circle of care, individuals will not in any way retrieve, copy, disclose, or transmit such information to any other individual or organization unless required for the care continuum. Individuals must hold in strict confidence all information obtained through their employment and must not disclose such information to any individual inside or outside the hospital **including their immediate family members.**

Breaches of this policy are considered cause for discipline, up to and including termination or loss of privileges or association with the Hospital.

Disclosure of Information – Staff Responsibility:
Disclosure of information is generally prohibited except in situations as outlined below:
- With either written or verbal consent from the patient whose information it is. Employees must confirm with all patients whether they want basic hospital information (i.e.: location, condition) released to the public.
- As necessary in the performance of current hospital duties.
- When failure to disclose information will place the patient or third parties in imminent danger.
- Pursuant to a court order, subpoena, summons, search warrant or other legislation.
- Access to one's own health record while in hospital or following discharge must be done in accordance with "patient access request to personal health information" policy.
- Access to employee's record in payroll/benefits coordinator's office as per appropriate policy and procedure.

Even when the health care professional is confronted with the necessity to disclose, confidentiality should be preserved to the maximum possible extent.

Enquiries by media:
All enquiries from the media, regardless of their nature, should be immediately referred to the Chief Executive Officer, or designate. After business hours, administration-on-call is to be contacted. All other enquiries that are not dealt with in this section (i.e.: police, lawyers) are to be referred to the Privacy Officer in conjunction with the Health Records Department. Every effort will be made to ensure confidential information is not inadvertently disclosed to persons not otherwise entitled to receive such information.

1. Subject to the **"reasonable limits"** described below, confidential information should never be discussed in any area where others not entitled to receive that information are present. For example:
    a) In public areas of the Hospital such as the elevator, stairwell, cafeteria, lounge

b) At home
c) In public places outside of the Hospital, unless required to do so by law or with permission from an authorized individual

2. Personal information/personal health information is not to be left in written form or displayed on computer terminals in areas or locations where unauthorized individuals may access it. Personal health information is not to be left unattended when there is no one to receive the information (i.e.: fax machines, photocopier) or when transporting patients with their health records.

3. Reproduction or copying of any personal health information will be limited and should not interfere with the integrity of the information. Staff reproducing or copying documents are responsible for ensuring that the documents are not left behind and that any discarded copies are disposed of securely (i.e.: shredding). Electronic/digital media will be disposed of by physical destruction (i.e.: breaking up CDs).

4. Filing cabinets, desks and storage areas that contain personal and personal health information will be locked when unattended. Keys to cabinets must be stored in a secure area away from the cabinets themselves.

5. Regarding faxing of personal/personal health information please see policy “transmission of personal health information by fax machines” policy.

6. The distribution/circulation of confidential documentation will be in sealed envelopes, addressed and marked ‘personal and confidential’.

7. Any information lost and found, deemed to be confidential, will be returned immediately to the appropriate area to which it belongs.

Reasonable Limits:
While every effort is made to maintain patient confidentiality, the Hospital recognizes that in practice reasonable limits may be placed on the principle of patient confidentiality and privacy. There are occasions where the provision of health care/education requires that confidential information be discussed among health care providers in patient care areas considered “public” in nature, open and accessible by the general public/other patients and hence, not private (i.e.” nursing stations, rooms with multiple patients, hallways, registration areas, etc.). The responsibility of the employee is to take reasonable and practical means of protecting patients’ privacy.

Role of employees:
Protect the privacy, confidentiality and security of personal and personal health information of patients, other employees. Responsibilities include:

- Reviewing hospital privacy policy and related procedures, information management and security policies and procedures related to their job functions.
- Employees should check with the Privacy Officer and/or manager when in doubt or if there are any questions/concerns.
- Practicing secure behaviours at all times (i.e.: discussion of personal health information only in private areas (cannot be overheard), not sharing passwords or posting passwords

where visible).
- New GDH employees must sign the confidentiality agreement as a condition of employment and be aware of the importance of maintaining confidentiality and the repercussions associated with a breach should a breach occur.
- Anyone becoming aware of fraudulent use of their access codes or authorization mechanisms must notify their manager and IS/IT Coordinator immediately.

Risk:
Breaches in the privacy or in the protection of personal information and personal health information at the Geraldton District Hospital could result in:
- Adverse consequences for the individual whose privacy has been breached.
- Adverse consequences for the employee.
- Breach of ethical guidelines and standards (includes Geraldton District Hospital mission, vision and values).
- Breach of professional ethics and standards of practice.
- Liability to the Hospital and/or health care provider.
- Negative impact on the Hospital reputation and public confidence.

Breach – What is a Breach?:
A breach includes any intentional or inadvertent unauthorized collection of personal health information, access to, or disclosure of, confidential information. It is not considered a breach to report patient information in a research study as long as the patient is not identifiable and follows appropriate research protocols. Individuals with reason to believe that you have breached or are about to breach or compromise privacy/confidentiality may complain to the Commissioner. Also, if the Commissioner learns of a possible breach on her own, a privacy review may be initiated.

All breaches are taken very seriously at the GDH. In the event of a breach, a consultation with the manager, Privacy Officer and CEO will occur to ensure a consistent and unbiased viewpoint. Human Resources consultant may be requested to provide potential disciplinary advice. Penalties for breaches will be assigned on a case-by-case basis. Depending on the facts involved in each case, disciplinary action may include a verbal or written warning, counselling, suspension, and termination of user privileges, termination of employment or affiliation with the GDH. Staff of professional colleges will be reported to their prospective college in accordance with the college's protocols for reporting data protection breaches. Breaches that are criminal in nature may involve the police. Documentation regarding all breaches will be retained in an individual's personnel file.

Reporting Breaches or Potential Breaches:
Hospital employees and affiliates have the responsibility to report suspected or known breaches of privacy, confidentiality and security to the immediate manager without fear of reprisal for doing so. All breaches must also be reported to the Privacy Officer.

Notification of potential breaches by the Director of Information Systems – Thunder Bay Regional Health Sciences Centre and St. Joseph's Care Group must be investigated as soon as possible as to the validity of employees accessing information in relation to patients, corporate personnel, etc. The Hospital, as a member of the Northwest Health Network, sharing a patient information database with other facilities, it is critical that reasonable care is

exercised not to access or disclose confidential information unless required in the performance of duties. Audits conducted periodically to confirm the appropriateness of access are conducted and any potential breaches are provided to the privacy officer for investigation. The summary of discussions and resultant disciplinary action (if any) with the employee must be submitted to the Director of Information Systems at Thunder Bay Regional Health Sciences Centre as per established procedures.

Containment of Breach:
Should a breach be confirmed, then the manager and Privacy Officer and/or Chief Executive Officer shall take immediate action to identify the extent of the breach and take steps to contain it.

Investigation of Breaches:
All alleged breaches will be investigated thoroughly to determine the nature and severity of the breach, if any. The manager, Privacy Officer, and support departments (i.e.: IS/IT), if necessary, will conduct an investigation. Discussions with employees will be held in the presence of their union representative, and per union collective agreement. A potential breach by a medical staff member will be brought to the attention of the privacy officer, who will address with Chief of Staff and Chief Executive Officer, where appropriate.

Notification of Breaches to Individual:
Upon confirmation of a breach then the Privacy Officer will take immediate steps to notify anyone whose privacy was breached. The notification will specify what and how much personal information/personal health information was affected. The communication will explain immediate and long-term steps the Hospital has taken to rectify the breach. Management, appropriate staff and the Hospital law firm (if required) re risk management are to be notified.

Corrective and Disciplinary Actions:
In the event of a breach, the existing Hospital procedures regarding corrective or disciplinary actions, in effect at the time of the breach will be utilized to address the issue. Depending on the nature and severity of the breach, employees may be subject to disciplinary action, up to and including termination of loss of privileges. Disciplinary sanctions may be reported to the applicable professional college or association, as appropriate. Should a member of the medical staff be the cause of a breach, then the Chief of Staff and/or CEO will assume responsibility in addressing the issue as required. A written warning may also be included as part of the Hospital's credentialing procedures.

Security level of breaches:
Breaches are divided essentially in the following three levels of severity:

Type 1- Carelessness:
Occurs when an individual carelessly accesses, uses or discloses personal information (i.e. patient health information, employee information) to other individuals (staff members or individuals external to the Hospital) who do not need to know the personal information. Examples include:

- When a user inadvertently accesses the wrong patient record (electronic)
- When a staff member discusses personal information in a "public" area without taking

reasonable precautions to avoid having unintended recipients overhearing
- When a staff member leaves patient or employee information (i.e. patient chart) in a public area
- When a staff member leaves a computer terminal with patient/staff information unattended whereby the information could be readily accessed by an unintended recipient

Type 2 – Curiosity and Concern:
Occurs when a staff member intentionally accesses or discloses personal information for purposes other than its intended/authorized use or for purposes other than to fulfill their job duties, but to satisfy their curiosity or concern. Several examples include:
- When a staff member accesses and reviews their own health record or their family member health record **directly** without going through the appropriate Hospital established processes to obtain such access. For example, the staff member reviews their on-line electronic health record, test results or medical reports directly, rather than obtaining such access via their care provider and/or Health Records department.
- When a staff member accesses and reviews a record of patient including family members, out of curiosity or concern, without prior expressed consent.
- When a staff member breaks the terms of the confidentiality agreement in that a user fails to log off the system when leaving it unattended, a user sharing his/her password with another user, a user accessing or requesting another user to access information on his/her behalf. This violation may also include a number of previous type 1 violations. There is no intention of personal gain by the user in a type 2 violation (this particular point relates to electronic access of the MediTech (Northwest Health Network) patient information database).

Type 3 – Illegal Use, Malice, Personal Gain:
Occurs when a staff member accesses, reviews or discloses personal information for personal gain, malicious intent or discloses/shares information with illegal intent. Some examples include:
- When a staff member reviews a patient record or staff record to use the information in a personal relationship or for personal gain.
- When a staff member uses information in a malicious manner (i.e.: to discredit an individual).
- For the MediTech (Northwest Health Network) patient information database, type 3 violation includes also when a user commits a type 2 violation accompanied by disclosure of information and/or with the intent for personal gain. This may also include a number of previous type2 violations.

Note:
The levels of breach in relation to MediTech (Northwest Health Network) violations as well as the disciplinary interventions are as per established protocols. The Privacy Officer is notified of any potential breaches via the regular audits, notification and reporting procedures.

Data security/protection of electronic information:
All GDH computer systems and much of the data/information residing on them are vital corporate assets. Individuals are responsible for protecting corporate data and information entrusted to them. Access must be appropriately authorized and granted on the basis of requirements to perform hospital responsibilities. Different layers of access require a unique

log-in ID and password. These include access via any remote virtual private network (VPN) or modem and a secure phone line, the LAN, computer applications/software, hospital voicemail system. All access layers, ID and passwords are controlled by the IT department. Employees must sign appropriate confidentiality and user agreements. See Appropriate Use of Technology policy and Confidentiality Agreement policy).

Orientation:
Review of policy and signing of confidentiality agreement. At the time of orientation, this policy and other privacy policies will be reviewed with all new hospital employees and affiliates and are required to sign a confidentiality agreement.

Changes to Employee Status:
Managers are required to notify the IT department of the GDH of any changes to an employee's status so that user accounts can be modified or deactivated, as required. This also requires the managers to inform the Payroll and Benefits Coordinator and Human Resources consultant of employee transfers, terminations, leaves of absence/maternity leaves. Employee ID badges are to be collected by managers, including any keys allowing access to specific areas within the hospital.

Information and Privacy Commissioner's Role:
Oversees privacy and freedom of information legislation in Ontario, including the Act. Under the Act, the Commissioner:
- Responds to privacy complaints.
- Initiates privacy reviews.
- Authorizes certain information collection practices, where appropriate.
- Educates and communicates with the public about health privacy.
- Researches issues affecting health privacy.
- Offers comments/advice on current or proposed information practices, on request.

Offence and Sanctions:
If you violate the law regarding a privacy breach, you may face:
- A Commissioner's order.
- A fine for an offence and/or a lawsuit for damages.

NOTE: Not all privacy breaches are subject to fines.

If prosecuted and convicted of an offence:
- The hospital or physician could be fined up to $250,000 or $50,000 respectively.
- The hospital's officers, members, employees or other affiliates who authorized or could have prevented the offence may be fined $50,000 whether or not the hospital itself is prosecuted or convicted.

A breach of privacy may entitle affected individuals to sue you for damages for:
- Actual harm a privacy breach caused.
- Mental anguish (up to $10,000) where wilful or reckless behaviour caused the breach.