E-ORIENTATION

WINDSOR
REGIONAL
HOSPITAL

OUTSTANDING CARE – NO EXCEPTIONS!

PRIVACY
&
CONFIDENTIALITY

PRIVACY & CONFIDENTIALITY

This course provides an overview of WRH corporate policies related to privacy and confidentiality. It outlines the importance of keeping patient health information private and confidential, and the professional expectations governed by legislation and hospital policy.

PRIVACY VS CONFIDENTIALITY

Confidentiality is the moral, ethical, legal, professional and employment obligation to protect the information entrusted to us.

Privacy is the right of an individual to determine when, how and to what extent they share information about themselves with others.

Personal Health Information Protection Act - PHIPA

STOP. THINK. PROTECT. Patient privacy is in your hands. www.ipc.on.ca

- Provides direction to all individuals who collect, use, disclose and retain personal information and personal health information (PHI)

- Under PHIPA, patient/substitute decision maker (SDM) have the right to:
    1. Access PHI
    2. Correct PHI
    3. Know who has accessed their information
    4. Challenge an organization’s privacy practices

- Includes: all staff, professional staff, volunteers, students and contracted staff at all healthcare facilities.

What is Personal Health Information?

Personal Health Information is identifying information in an oral or recorded form.

Any information that connects patients and their care to their hospital, clinic or care team is Personal Health Information.

Examples:

- Date of birth, address
- Medical Record Number (MRN), OHIP Numbers
- Records from previous visits
- Name of Health Care Provider
- Family History
- All information related to physical or mental health

What is Confidential Information?

WRH considers the following types of information to be confidential

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- Information regarding WRH operations, which are not publicly disclosed by WRH (e.g. unpublished financial statements, legal matters, quality of care)

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

Role of the Privacy Team

- Advocate for patient and staff privacy within the organization
- Act as the privacy experts
- Facilitate implementation of privacy laws and principles
- Conduct internal audits of health records and the organization's processes to ensure compliance
- Develop privacy related policies and processes

What is appropriate access? Access to health information is based on "need to know" and circle of care guidelines

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 WRH 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 information through the organization's release of information process in the Health Records Department

continued

What is appropriate access? Access to health information is based on “need to know” and circle of care guidelines

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 duties

When used for purposes other than 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 Records Department. Other uses can also include authorized access by Legal Affairs/Human Resources or designated management staff to ensure compliance with this policy and legislation.

What is Inappropriate Access?

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

10 PRINCIPLES FOR USING INFORMATION

Accountability:

This is the responsibility of the organization for the information under its control

Identify Purpose:

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

Consent:

Consent is required from the patient to collect, use, share and retain information. Implied consent is used for most core activities of the hospital.

Limit Collection:

Collect only information that is necessary to accomplish the intended informed purpose.

Limit Use and Retention:

Information may be used only for the purposes for which it was collected, except with consent or as required by law. It is retained only as long as necessary.

10 PRINCIPLES FOR USING INFORMATION

Accuracy:
Patients have the right to request corrections or amendments to their records, if they feel they are inaccurate.

Safeguards:
Organizations must implement appropriate safeguards to protect personal information against loss.

Openness:
To be open and honest with patients and the community regarding information management practices.

Individual Access:
Patients have the right to access their information including viewing or requesting a copy of their record.

Provide Recourse:
Patients have the right to express their concern regarding our information practices including taking their concerns directly to the Privacy Commissioner of Ontario.

How to Maintain Confidentiality

- ***Conversations:*** Discuss information in private areas NOT in public areas (cafeteria, elevators, other patient rooms).
- ***Email Usage:*** Do not email confidential/sensitive information.
- ***Computer Etiquette:*** Do NOT share your password. Always log-off your computer or lock your workstation. You are responsible for activity under your password.
- ***Physical Storage:*** File information or put charts away in their proper place. Wear your ID Badge, question unescorted strangers, transport charts or other PHI face down or in envelopes and NEVER leave charts unattended.
- ***Leaving Messages:*** When possible, obtain consent to leave messages. Determine how your patient wants to receive communication. A message should only include your name and phone number - not where you are calling from or why.

Remember where you work. Do not relay or identify to others when you see family, friends, neighbours, etc. at the hospital.

Verbal & Telephone Requests for Information

Basic hospital information (location and phone number) will be given out upon 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.

Unless the patient/SDM have placed restrictions, information that may be released without consent or warrant includes:
A) the absence or presence of the patient in the hospital
B) a condition update of the patient

Sending Confidential Information

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 Department for cases where an urgent and immediate transfer is required.

The original chart is NOT to leave the building.

Select the most secure method of sending hard copy and transmitting electronic confidential information.

- If you need to send confidential information outside the organization for your role, either re-identify the info, encrypt the file or send in a secure manner e.g. Secure File Transfer
- E-mail is NOT a secure manner of sending information outside the organization.

Information Security

Position computer screen in such a way that unauthorized individuals cannot "shoulder surf".

Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information.

Store electronic confidential information on hospital network drives, not on local hard drives or portable devices unless necessary and if so, use additional security measures.

Do not post confidential information on personal or public web pages e.g. blogging, social media, internet messaging.

Dispose of printed confidential information by putting it in the confidential waste receptacles or by shredding the documents.

Confidential information requiring shredding includes the following:

- Health Care Information
- Quality Assurance Information
- Business Information
- Employee Health Records
- Any other information deemed confidential (this includes ALL personal identifiers)

STOP. THINK. PROTECT.
Patient privacy is in your hands. www.ipc.on.ca

In clinical areas do not leave the chart box open and unattended. To maintain confidentiality, always close the chart box before leaving the charting station.

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.

- Regular Audits will be conducted monthly and reviewed by the Privacy Team on randomly selected patients
- Ad Hock Audits can be requested by a member of Executive or Senior Management Team, Legal Affairs/Risk Management, Human Resource Department, Physician Leader or Patient Representative on behalf of patient (including staff who are patient).

PRIVACY & CONFIDENTIALITY

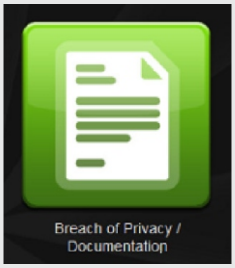
A Breach of Confidentiality

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 the Privacy 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.

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

Did You Know?

A Breach of Privacy/Confidentiality can be reported using our RL6 Reporting Software. All reports of a breach of privacy should be entered into RL6 before the end of your shift. Please look for this icon on the icon wall.



Department managers, in conjunction with Human Resources and/or Legal Affairs/Risk Management depending on personnel involved will investigate alleged breaches. If allegations are substantiated, the individual may be subject to disciplinary action up to and including termination of employment/contract or loss of privileges or affiliation with WRH.

Steps in the Management of a Privacy Breach

1 **Step 1:**
Contain the breach or secure the PHI to reduce the likelihood of a breach

2 **Step 2:**
Investigate the potential/actual breach and evaluate the risks associated with the breach

3 **Step 3:**
Notify all those affected by the breach

4 **Step 4:**
Manage the risk of future breaches

PRIVACY & CONFIDENTIALITY

Before collecting, using or disclosing Personal Health Information (PHI) - **STOP** and ask yourself these two questions:

1. Do I need to access this information to care for the patient?

2. Do I need to share this information to care fo the patient?

If you've answered **NO** to either question, you should not access or share the information to avoid breaching the patient privacy rights!