

E-ORIENTATION



PRIVACY & CONFIDENTIALITY

PRIVACY & CONFIDENTIALITY



This course provides an overview of 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.

Our position as a Health Care Team requires that we have access to patients' **private** information, and that they trust that we will treat it **confidentially**.

Personal Health Information Protection Act - PHIPA

- 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

PRIVACY & CONFIDENTIALITY

What is Confidential Information?

WRH/HDGH 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- Information regarding WRH/HDGH operations, which are not publicly disclosed (e.g. unpublished financial statements, legal matters, quality of care)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/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 information through the organization's release of information process in the Health Records Department

continued

PRIVACY & CONFIDENTIALITY

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

1. Accountability:

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

2. 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

3. 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.

4. Limit Collection:

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

5. 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

6. Accuracy:

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

7. Safeguards:

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

8. Openness:

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

9. Individual Access:

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

10. 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.

Express vs. Implied Consent

Express Consent

Express consent is given either verbally or in writing, to a health information custodian (HIC) to collect, use or disclose your personal health information. Except in circumstances where PHIPA permits the collection, use or disclosure without consent, express consent is required if:

- Personal health information is disclosed to a person or an organization
- Personal health information is disclosed by one HIC to another for a purpose other than providing or assisting in providing health care
- A HIC collects, uses or discloses personal health information for the purpose of marketing or market research
- A HIC collects, uses or discloses personal health information for the purpose of fundraising

Implied Consent

Implied consent is not defined in PHIPA; however, it is understood to be consent that one concludes has been given based on what an individual does or does not do in the circumstances. A HIC is not required to obtain written or verbal consent every time personal health information is collected or used in the course of receiving medical care. It may be reasonable for the HIC to conclude that consent has been given to the collection or use of personal health information because of certain things that occur while delivering care. For example, when a patient consents to a physician issuing a prescription, it may be reasonable for the physician to conclude that there is implied consent to the disclosure of personal health information to the Pharmacy for filling the prescription.

PRIVACY & CONFIDENTIALITY

Withholding Consent

Just like it is possible to provide express consent, it is also possible to expressly refuse or withhold consent to the collection, use or disclosure of personal health information. If consent is withheld or not given, then the health information custodian cannot collect, use or disclose the patient's personal health information unless PHIPA otherwise allows the practice without consent.

Consequences

The need to protect the privacy of individuals' personal health information has never been greater given the:

- **Number of people involved in the delivery of care**
- **Involvement of multiple organizations**
- **Increased portability of PHI**
- **Emphasis on information technology and electronic exchange of PHI**

Consequences of Inadequate Attention to Privacy Information Security

Discrimination, stigmatization and psychological or economic harm to individuals based on the information

Individuals being deterred from seeking testing or treatment

Individuals withholding or falsifying information provided to health care workers

Loss of trust or confidence in the health care system

Costs and lost time in dealing with privacy breaches

Legal liabilities and ensuing proceedings

Circle of Care

The term “circle of care” describes the ability of certain health information custodians to assume a patient's implied consent to collect, use or disclose personal information for the purpose of providing health care

The circle of care may include doctors, nurses, pharmacists, allied health professionals, clerks and any other individuals involved in a patient's care. Individuals not part of a patient's direct or follow-up treatment are not included with the circle of care

PRIVACY & CONFIDENTIALITY

You are permitted to release information to other providers unless a patient has told you they do not want their information released to that person/facility

Access only the information that is essential for you to do your own work. Written consent is required for an individual to view their own records

Consent to share information with providers in the circle of care is generally implied. A patient who accepts a referral to another healthcare provider implies consent for sharing relevant information. This includes sharing with physicians and other healthcare providers who are caring for the patient, but does not include others such as family, police, etc.

Steps to Maintain Confidentiality

Think About It!

Before collection, using or disclosing 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 for the patient?



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

Conversations

Discuss information in private areas NOT in public areas (cafeteria, elevators, other patient rooms).

Email Usage/Security

- Email is a record for the purposes of the Freedom of Information and Protection of Privacy Act, and thus may be accessible to others under certain circumstances for review and release
- Email usage may be subject to public scrutiny and/or disclosure
- Do not email confidential/sensitive information to accounts external to the organization's secure system e.g. hotmail. Cogeco, gmail, yahoo, etc.
- When sending messages to authorized individuals or companies outside of the hospital, everyone must keep in mind that emails sent externally are not secure
- Messages sent via the Internet are stored on various systems and servers over which the hospital has no control, and therefore they may be read voluntarily or involuntarily by unintended recipients
- If you intend to send confidential or sensitive hospital business outside the hospital system, you must contact the Transform Help Desk to verify the security of the email address.
- All emails must include the hospital confidentiality disclaimer. Review each hospital's *Electronic Mail Usage* policy for more information

PHI on Mobile Devices

- There should be NO PHI stored on any mobile device. If you feel that something needs to be on a device, you should contact WRH/HDGH's Privacy Officer
- All healthcare practitioners, staff and other agents must ask themselves one key question before copying any health information to a mobile device "Is it necessary to store personal health information on this device?"
- If the answer is "yes", consult the Chief Privacy Officer and, if necessary, the information will be encrypted and de-identified by removing all personal identifiers

Note: Fingerprint identification is NOT considered foolproof or secure

PRIVACY & CONFIDENTIALITY

Computer Etiquette

- Do NOT share your password. Always log-off your computer or use your tap-and-go card (if applicable) to log off of your workstation on wheels (WOW) when not in use
- Remember that you are responsible for activity under your password
- Try and position your computer screen such that unauthorized individuals cannot peek over your shoulder and monitor your screen (shoulder surf)
- Store electronic confidential information on hospital network drives and not on local hard drives or portable devices, unless necessary and, if so, use additional security measures

Physical Storage

- File information or put paperwork away in its proper place
- Wear your ID Badge
- Question suspicious unescorted strangers
- Transport pieces of PHI face down or in envelopes and NEVER leave paperwork or screens unattended.
- Dispose of printed confidential information by putting it in the confidential waste receptacles or by shredding the documents

Leaving Messages

- When possible, obtain consent to leave messages
- Determine how the patient wants to receive communication
- A message should only include your name and phone number - not where you are calling from or why

Other good practices

- Access only the information/records needed to do your role in the organization
- Just because you have access to the electronic patient record system does not mean you can access any record, even if it is kept confidential. This includes records of family, colleagues, etc.
- Remember where you work. Do not relay or identify to others when you see family, friends, neighbors, 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

PRIVACY & CONFIDENTIALITY

Information Security Tips

Do not take pictures or screen shots of live patient data

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

If you are demonstrating a system to a colleague in person or via webinar, do not use live patient data

If you must share information with a system vendor for troubleshooting purposes, remove any identifiable information. If in doubt, contact the hospital's Privacy Officer

If you have to print PHI, follow procedures for labeling, storing and destroying the information once not needed

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)

In clinical areas do not leave the patient paperwork unattended. To maintain confidentiality, always tap out/log out of the electronic chart before leaving the WOW..

Audits - Random

- WRH/HDGH will randomly conduct audits on patient records to ensure information is being accessed only to appropriate personnel and for the right reasons
- 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 any health care provider who is a patient)
- You are expected to cooperate when contacted regarding the circumstances of access
- Do not access your own records or those of a family member – requests must be fielded through Health Records

Did you know? Patients can request for their records to be locked

- Follow WRH/HDGH procedures to get the lock/unlock in place and record the request. Patient information will be locked upon discharge
- The request will be coordinated with other institutions who share the system
- Physicians will be able to override a locked record to prevent imminent harm to a patient. They will follow local procedures and submit requests to the Privacy Officer or Health Information Management department and should include comments regarding the circumstances that required the override



PRIVACY & CONFIDENTIALITY

Same Name Searches in Cerner

WRH/HDGH prides itself on its strong privacy practices. The Cerner system (electronic charting) has a robust and thorough auditing solution known as P2 Sentinel to assist in identifying potential breaches of privacy. This auditing tool has a number of real-time notification features that include notification for all “**same patient name searches**” and “**same last name searches**”.

What is a “Same Patient Name Search”?

This is when a user searches their own chart in Cerner.

What is a “Same Last Name Search”?

This is when a user searches the chart of a patient with the same last name as them.

Under no circumstances is a user allowed to search their own chart or the chart of a relative (ie. spouse, child, parent, etc.) in Cerner.

These are serious breaches of privacy and will be reported to Human Resources and perhaps to the Information and Privacy Commission of Ontario (IPC).

If you are legitimately accessing the chart of a patient with the same last name as you, you should enter a comment into Powerchart while you are in the chart

If you would like access to your own chart, you are entitled to it just as any patient is. The process for production of your health record is by way of a request to Health Records, it is not by searching your own chart. WRH/HDGH is committed to maintaining its strong privacy practices and will investigate all improper searches.

If you have any questions about patient privacy please reach out to your Manager, Director or to the Chief Privacy Officer.



PRIVACY & CONFIDENTIALITY

A Breach of Confidentiality

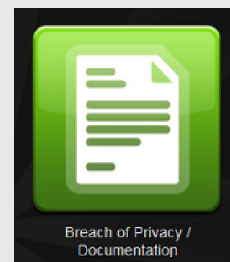
A breach of confidentiality includes any inadvertent or intentional collection, use and/or disclosure of personal health information, whether verbal or written, in breach of the Privacy Policy. Every person working at the Hospital has the right and responsibility to report a breach of confidentiality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

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

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

Consequences of Breaching Confidentiality

Hospitals have a responsibility to ensure confidentiality is maintained by staff and affiliates. Failure to maintain confidentiality may result in disciplinary action, including:



*PHIPA includes personal fines up to \$100,000 that may be applicable for those ignoring the privacy legislation and failing to maintain confidentiality



PRIVACY & CONFIDENTIALITY

Security Essentials

Securing Devices and Data in Public

- Be cautious about open Wi-Fi networks – free and open access Wi-Fi networks are NOT secure
- Before connecting, make sure a network is legitimate. Scammers create “rogue” and “evil twin” networks to fool users
- When logging into email or other secure sites, be sure to use *https* to keep your communication safe

Mobile Communications

- Only communicate with trusted sources – that goes for texting, phone calls, Bluetooth devices, etc.
- Only download apps you trust. Permissions, reviews and other information can reveal danger signs. If you're not sure, don't download
- Think before “checking in” on social media. These activities can reveal your habits to scammers

Be mindful of your Surroundings

- Keep devices with you at all times. A laptop, phone or tablet could be snatched up in a moment
- Shield login screens and other sensitive content from prying eyes
- Avoid video chats and private conversations in public areas. Don't discuss anything personal or confidential that shouldn't be overheard

Securing the Workplace

- Access to secure areas should be restricted to authorized individuals

Maintain the Integrity of Audit Trails

- Keep ID's, badges, keys and fobs secure – don't lend or borrow credentials
- Understand that, if others use your credentials, you are on the audit trail
- Always scan your badge or ID at a secure entrance, even if the door is held for you
- Remind others to scan IDs when they enter

Know Who and What Belongs

- Scammers seek opportunities to access secure places and systems
- Do not give strangers without proper credentials access to secure areas
- Alert Security to any “abandoned” items in the workplace e.g. ID's/badges, USB drives (which could be infected with malware), packages and/or any unusual items

Keep it Simple

- Make sure secure doors close and latch behind you
- If a secure door is propped open or damaged, or if you see someone or something else out of the ordinary, report it to your manager and/or security

PRIVACY & CONFIDENTIALITY

Securing Corporate Data and Systems

There are a number of potentially risky situations employees could face on any given day

Keep Private Information Private

- Do not share sensitive information with strangers or other unauthorized sources
- Keep confidential papers, files, plans and other details out of public view
- Do not discuss sensitive topics in conversations that could be overheard
- Keep login credentials private and do not sign into systems for your coworkers

Use physical and technical safeguards

- Lock your systems and safely store devices when you leave your desk/work area
- Use complex passwords and vary them from system to system
- Destroy unwanted documents, CD's and other storage media that contain sensitive data
- Use encryption when storing or sharing files that contain confidential information

Be aware of social engineering techniques

- Phishing emails are a common threat, so think before you click; even messages and attachments from coworkers could be dangerous if their accounts have been hacked
- Smishing attacks – malicious SMS/text messages – tempt you to click dangerous links or reveal personal data
- Vishing (short for “voice phishing”) calls are used by social engineers to get you to share private information

Working Safely Outside the Office

There are some unique risks that are introduced in remote and home office environments

Keep Devices and Connections Safe

- Use passwords, swipe patterns or other locks on all business and personal devices
- Enable security measures – system passwords, firewalls, anti-virus software, etc., on your home networks, particularly wireless systems
- When possible, use a corporate VPN to establish remote connections to business systems

Set Boundaries for Data

- Be cautious about removing sensitive files and information from your corporate office
- Do not store confidential business data on your personal devices
- Limit the amount of personal content you place on business devices
- Do not allow friends, spouses or children to use corporate devices or accounts

Stay alert and cautious when online

- Be smart about what you click and download
- Shortened URLs can hide dangerous links
- Pop-ups and ads often contain malware
- Dangerous apps and files can compromise your data and devices
- Pirated content is particularly dangerous (and illegal)