



Privacy and Confidentiality Annual Training for Volunteers

The purpose of this course is to help you gain a better understanding of the privacy principles. We will look at how we can apply these principles everyday at work and outside of work. The intention is to reduce privacy issues and breaches by outlining strategies to help you maintain confidentiality and protect information.

- ≡ **Welcome!**

- ≡ **Personal Health Information (PHI)**

- ≡ **PHIPA and FIPPA**

- ≡ **The Circle of Care and Consent**

- ≡ **How does the Hospital protect information?**

- ≡ **How can YOU help protect information?**

- ≡ **What information can you share?**

- ≡ **Privacy Breaches**

☰ Privacy & Social Media

☰ Know YOUR Responsibilities

☰ Privacy Pledge

📄 Final Quiz

☰ Thank you!

QUESTION BANKS

Welcome!




Welcome to the Annual Privacy & Confidentiality training for Volunteers at Grand River Hospital

What is Privacy?

Privacy is a **RIGHT** that is protected by law and gives an individual control on how, when and to what extent their information will be shared with others.

What is Confidentiality?

Confidentiality is a hospital's **OBLIGATION** to ensure privacy by limiting access and disclosure.



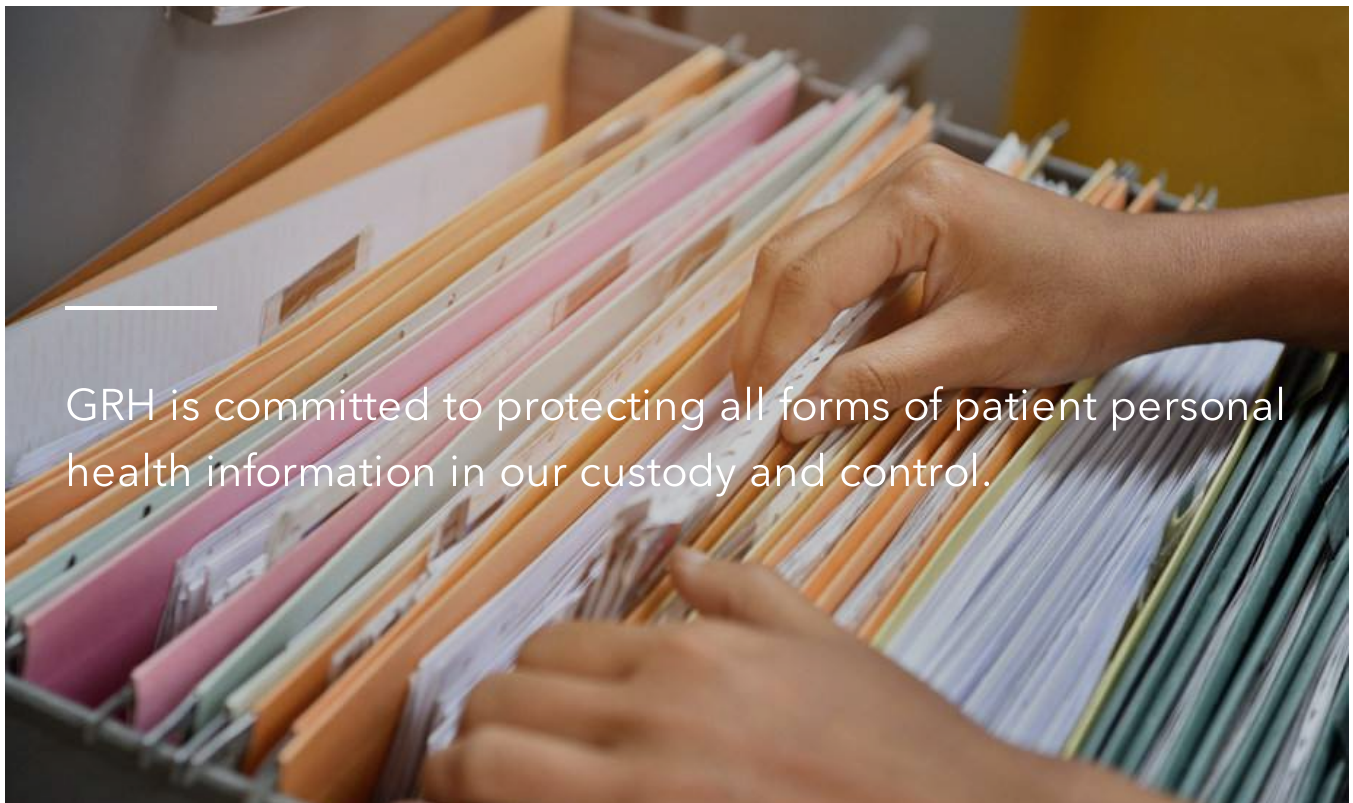
The purpose of this course is to help you gain a better understanding of the **privacy** principles and your accountability for handling patient information and maintaining **confidentiality**. We will look at specific and practical strategies to help you apply these regulations everyday to reduce the risk of privacy issues and breaches.

Please note: This course contains several hyperlinks to policies and other information on Lotus Link that will not work if you are taking this course from home. To access these hyperlinks you would need to be at the hospital and connected to the network.



GREAT! LET'S GET STARTED!

Personal Health Information (PHI)



GRH is committed to protecting all forms of patient personal health information in our custody and control.

What is Personal Health Information (PHI)?

Personal Health Information (PHI) includes any identifying or *potentially* identifying information in any form, e.g. written, read, observed, or heard at the hospital.

This includes any information about a patient, such as their name, address, phone number, next of kin, tests, diagnosis, treatment, or discharge plans.

In addition, it may also includes ambiguous information that could *potentially be* identifying when combined with other publicly available information, e.g. through social media, other media publications or web searches.

Anyone who has the right to access PHI in the course of their work, has an ethical and professional obligation to protect the confidentiality of the information and to access and use only as required in their work.

All staff and volunteers are expected to implement good security practices consistent with the value of the information.

NEXT LESSON

PHIPA and FIPPA

P

Personal

H

Health

I

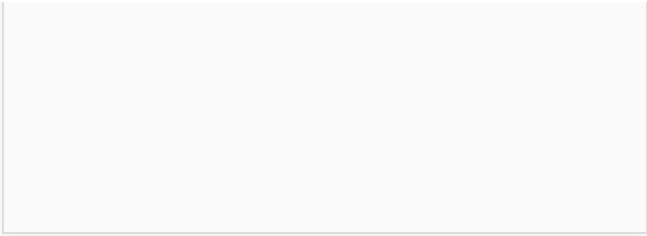
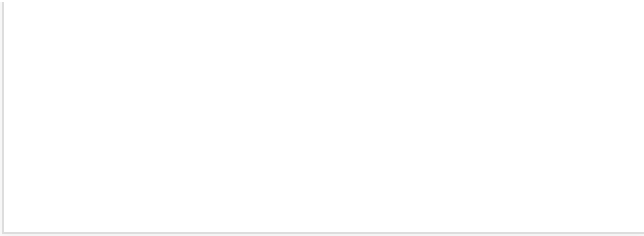
Information

P

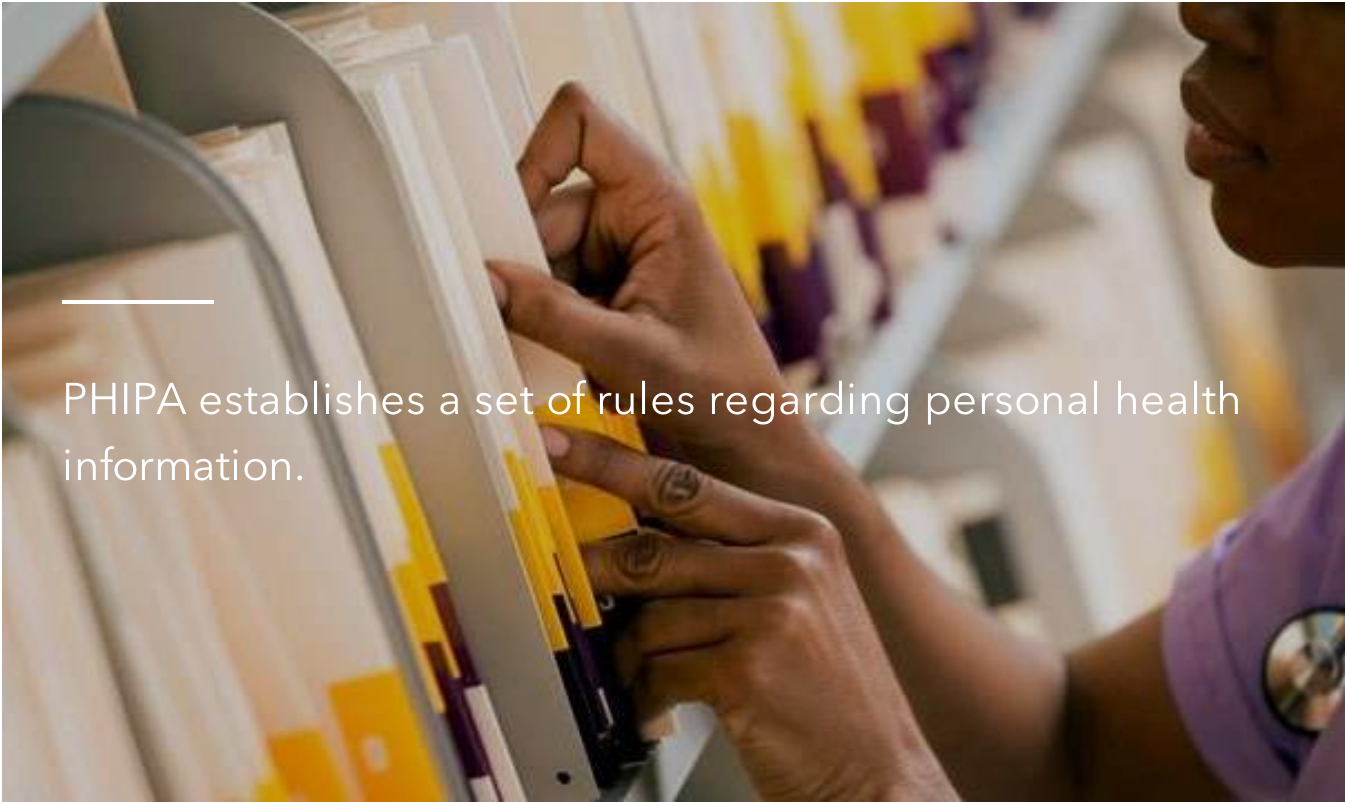
Protection

A

Act



The Personal Health Information Protect Act (PHIPA) is a provincial law regulating the management of personal health information. It regulates how patients' information is collected, used and disclosed. Under this law, patients have greater control over their information and hospitals are held accountable for notifying patients of privacy breaches.



PHIPA establishes a set of rules regarding personal health information.

PHIPA gives patients the right to:

- be informed of the reasons for the collection, use and disclosure of their personal health information;

- be notified of the theft or loss or of the unauthorized use or disclosure of their personal health information;
- refuse or give consent to the collection, use or disclosure of their personal health information, except in certain circumstances;
- withdraw consent by providing notice;
- expressly instruct that their personal health information not be used or disclosed for health care purposes without consent;
- access a copy of their personal health information, except in limited circumstances;
- request corrections be made to their health records;
- and complain to the Information and Privacy Commissioner (IPC).



Frequently Asked Questions *Personal Health Information Protection Act*

September 2015



The [PHIPA \(Personal Health Information Protection Act\) Frequently Asked Questions](#) guide, pictured to the left, provides comprehensive information including:

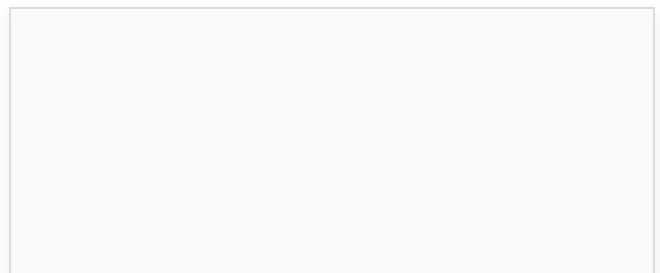
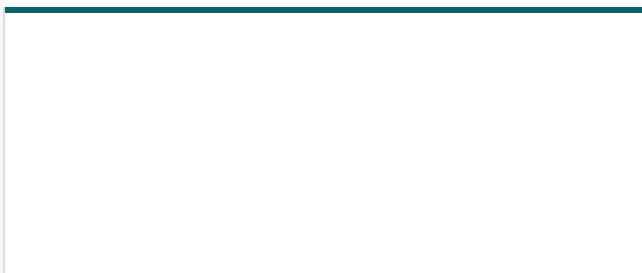
- interpretation and application of PHIPA
- practices to protect PHI
- consent concerning PHI

- collection, use and disclosure of PHI
- fundraising and marketing
- research
- Ontario health cards and health numbers
- access to records of PHI and correction
- administration and enforcement

[CONTINUE](#)

Let's turn our attention now to another piece of important privacy legislation, The Freedom of Information and Protection of Privacy Act (FIPPA).

[TELL ME MORE!](#)



F

Freedom of

I

Information and

P

Protection of

P

Privacy

A

Act

FIPPA is a provincial law that allows the public to request any hospital record, except personal information/personal health information of patients and staff (e.g. employment info).

Be aware that all documents you create in your role at the hospital may be requested including handwritten notes on documents, voicemails, emails, incident reports etc.

NEXT LESSON

The Circle of Care and Consent

What is 'The Circle of Care'?

The 'circle of care' refers to those individuals who directly provide or assist in the care or treatment of a particular patient at a particular point in time and **need to know** the information to provide or help to provide care to the patient.

This includes but is not limited to: doctors, nurses, technicians, therapists, individuals who work at community care access centers, or out-patient services.

The circle of care does NOT include lawyers, insurance company representatives, police officers and most other third parties.



Are volunteers part of the circle of care?

Volunteers play a very important role in enhancing the patient's experience. Although they are NOT considered to be in the Circle of Care (as they do not plan or provide direct care), volunteers work closely with those directly involved in patient care.

CONTINUE

What is Consent?

Consent is the permission from a patient or substitute decision maker (SDM) to collect, use or disclose their personal health information.

There are two forms of consent: **Express Consent** and **Implied Consent**.

Express Consent:

Express Consent is permission that's given specifically, either verbally or in writing, to allow or disallow the collection, use or disclosure of personal information.

Staff need to get express consent before they can access or share personal health information with people who are not within the patient's "Circle of Care".

Implied Consent:

Implied Consent on the other hand, is an assumption of permission that is inferred from a individual's actions or the presenting circumstance. Personal health information can be released to those in the "Circle of Care" for the provision of care based on implied consent.

For example, if a person comes to the emergency department we can rely on implied consent that the person is seeking treatment and is also consenting to the use of his/her personal information in order to provide or plan for that treatment.

If you have questions about consent or if you are asked to provide information in your role as a Volunteer, please refer to your staff contact person for assistance.

NEXT LESSON

How does the Hospital protect information?



The hospital has **Technical, Administrative** and **Physical** measures in place to protect the information in its custody from inappropriate collection, access, and disclosure.

Let's look at some examples of the measures we use.

CONTINUE

Technical Measures

• *Login passwords* • *Limiting access to data / information* • *Firewalls* • *Audits*

Technical measures that we have in place include login passwords, firewalls and limiting access to our systems to only people who require it. For example, logging-in when you use patient locator is a technical control to limit access to that system.

Administrative Measures

• *Privacy policy & procedures* • *Mandatory privacy training* • *Confidentiality agreements* • *Record retention & destruction practices*

The hospital has important policies and procedures in place to help maintain privacy and confidentiality. This e-learning course and the confidentiality agreement that you will find at the end are also administrative measures that the hospital employs.

Physical Measures

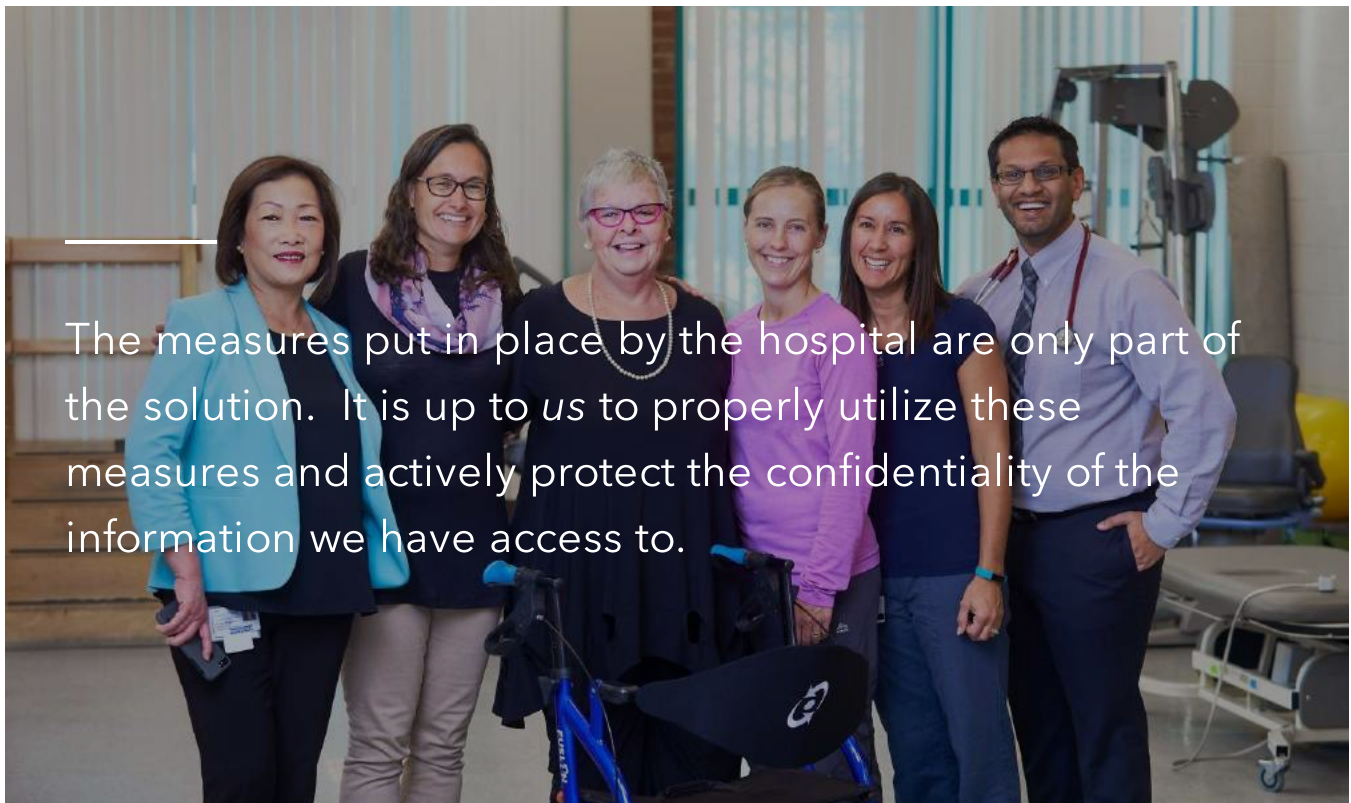
• *Secure storage* • *Locked filing cabinets* • *Restricted access to offices* • *Secure workstations*

Physical measures are also very important in maintaining privacy and confidentiality. For example, locked doors, privacy walls, and confidential shredding bins are all physical measures that the hospital has in place to help ensure that patient information is not viewable or overheard by the public.

Some physical measures you are expected to implement in your day to day work include; carrying patient lists on a clip board with a coversheet and locking-up or shredding any PI/PHI at the end of your shift.

NEXT LESSON

How can YOU help protect information?



The measures put in place by the hospital are only part of the solution. It is up to *us* to properly utilize these measures and actively protect the confidentiality of the information we have access to.

Let's have a look at some strategies that you should use...

- Remember to only access the computer system under your own credentials and log off when finished
- The 'circle of care' applies to information in our electronic systems. Think about what role you are performing and what access you've been given. Does it make sense? Ask for clarification if you need to.
- Don't EVER share passwords! Passwords should only be provided by designated staff. If you or another volunteer forgets your password, please refer to your staff contact.
- GRH only allows approved encrypted USB sticks, do not bring your own USB stick from home.
- Do not save PHI on portable devices
- Refer to GRH's Acceptable Use of Information Technology Assets Policy for more information.

2

Administrative Strategies:

- Know our privacy policies and procedures! These include policies to protect against unauthorized use of PHI.
- Be sure you read and understand our Confidentiality Agreement - you will encounter this annual attestation at the end of this course!
- Complete this e-learning on an annual basis to keep the information front of mind.
- GRH has a No Photography, Video and Audio Recording Policy. There are signs throughout the hospital indicating this. It is in place to protect the privacy of patients, staff and volunteers. Acceptable use of these devices is only warranted under certain circumstances: there is no PI/PHI in the background and everyone captured in the recording has consented to be there.

3

Physical / Behavioral Strategies:

- Avoid speaking about confidential information in a public area or outside of GRH with your friends or family. Even when not using names, you should never talk about a patient's care in elevators, the

coffee line, or other public places.

- If you see someone you know at the hospital, do not ask them the reason they are here. Instead, you can lead with "Hello, it's good to see you!" and let them know that you will not share with anyone the fact that you saw them at the hospital.
- Don't need it? Don't read it! You have access to information only as necessary to fulfill your volunteer role at GRH. Use only what you need, and don't look up any information that you don't need.
- Do not take PHI off of the floor/unit. For example, be sure to empty your pockets of any PHI and dispose of it appropriately before leaving.
- Use the designated grey confidential bins (pictured below) to dispose of PHI, not the blue recycle bins or the garbage cans.



**Remember - What happens at
GRH, stays at GRH!**





NEXT LESSON

What information can you share?



We have learned how we can work to keep information confidential, but what information *can* you share with people who are outside of the circle of care?

The Privacy Code and Opt-Out

If the individual has the first and last name of the patient but does not have the privacy code, volunteers can release the following information unless the patient has opted out of the patient directory (see [Patient Directory Opt-Out policy](#)):

- Confirm patient presence at the hospital;

- Disclose the patient's general location (i.e. in the ED); and
- Describe the individual's general health status (fair, good, satisfactory)

If the individual has the first and last name of the patient and the privacy code you can release the following information (see [Privacy Code Policy](#)):

- Confirm patient presence at the hospital;
- Disclose the patient's location and room number;
- Describe the individual's specific health status

How should I respond to inquiries about patients via telephone?

There are several things that you can do to respond to phone call inquiries. If the patient did not opt-out of the patient directory you can transfer the call to the patient. Or you can simply take the caller's name and phone number and give it to the patient to call back.

Know that if the patient has provided the individual with the 4-digit "privacy code", then you can provide personal health information.

How should I respond to inquiries about SMGH patients ?

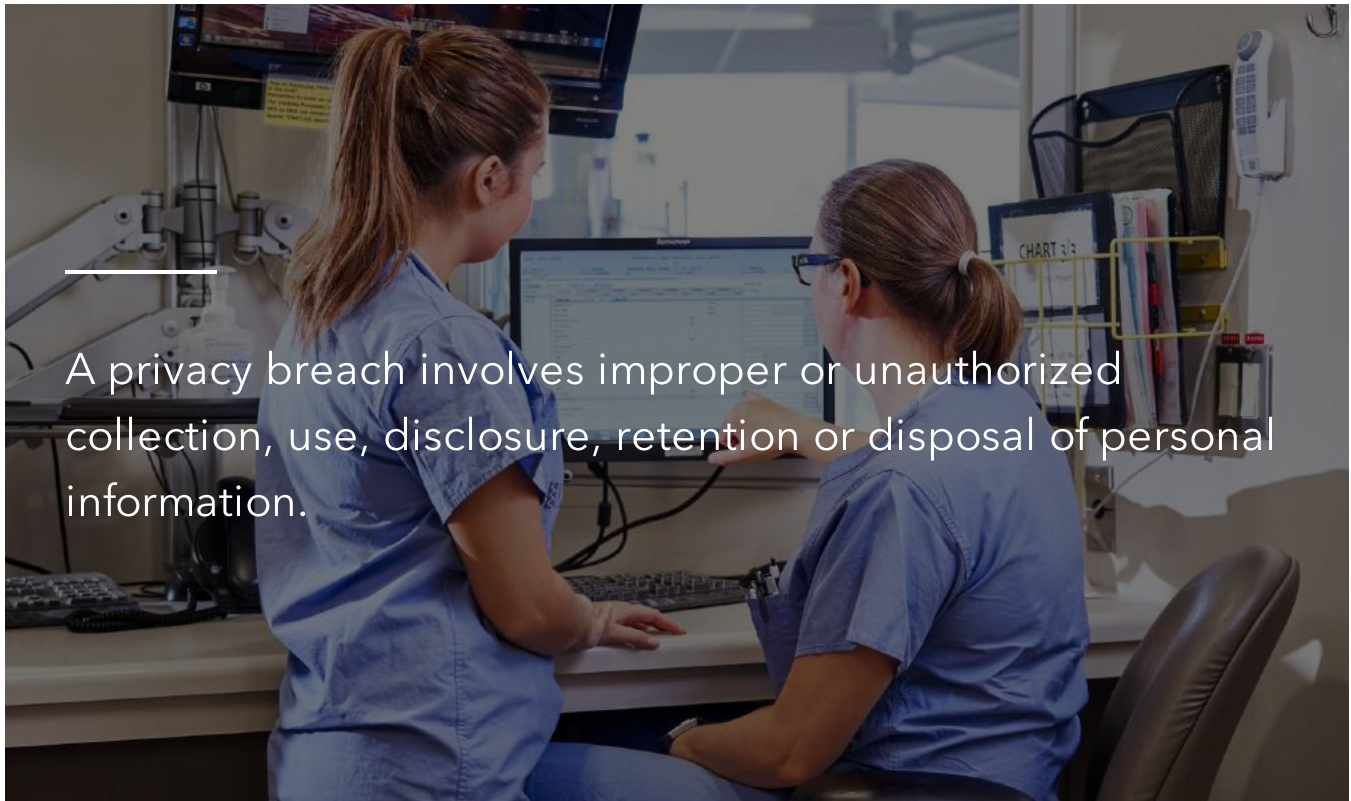
Our new electronic system has introduced wonderful opportunities between Grand River Hospital (GRH) and St Mary's General Hospital (SMGH). However, it is important to note that while you are fulfilling a role at GRH, you are not to release information about SMGH patients. If someone inquires about a patient, and you see they are not at GRH but instead at SMGH, you cannot share this information. Simply reply, "There is no patient with that name here."

What information can I release to the Police?

Volunteers should not provide the police with any information, and instead refer the officer to a staff member.

NEXT LESSON

Privacy Breaches



A privacy breach involves improper or unauthorized collection, use, disclosure, retention or disposal of personal information.

A breach of legislation, policy or confidential information may occur:

- 1 When PHI or PI is collected, used, or disclosed in a way that is not in accordance with legislation or hospital policy.
- 2 When PHI/PI is stolen, lost, or subject to unauthorized copying, modification, retention or disposal.

3

Where the privacy provisions in contracts, data sharing, or research agreements have been contravened.

4

Through failure to secure and protect confidential business information (i.e. employment contracts, financial information).

What happens if I discover a Privacy Breach?

If you become aware of patient information being lost, stolen, shared or accessed by an unauthorized person, you have a duty to notify a staff member as soon as possible.

If you find what looks like PHI, pick it up and give it to a staff member for them to deal with appropriately.

What are the consequences of a Privacy Breach?

If there is a deliberate breach of information, the individual may be facing disciplinary action such as loss of employment, loss of volunteer position, substantial personal fines, or even imprisonment in severe cases.

Breaches of confidentiality may also result in the loss of patient/family trust, and have negative impacts on the hospital's reputation.

NEXT LESSON

Privacy & Social Media



We encourage staff and volunteers to use social media on your own time, and to please be respectful of patient, staff and visitor privacy at all times when engaging in social media.

We understand the importance and value that social media has for community engagement, professional development and interaction with others. Staff members, physicians and volunteers who use social media are asked to use it appropriately.

Social Media Do's

- Do - Honour your personal reputation.
- Do - Respect the privacy of patients, visitors and other staff members.
- Do - Be accountable in your use of social media and aware that it can positively or negatively reflect your personal reputation.
- Do - Respect your hospital's brand, reputation and values.
- Do - Consider yourself a representative of the hospital at all times. What you say online and offline reflects on you and the hospital.

Social Media Dont's

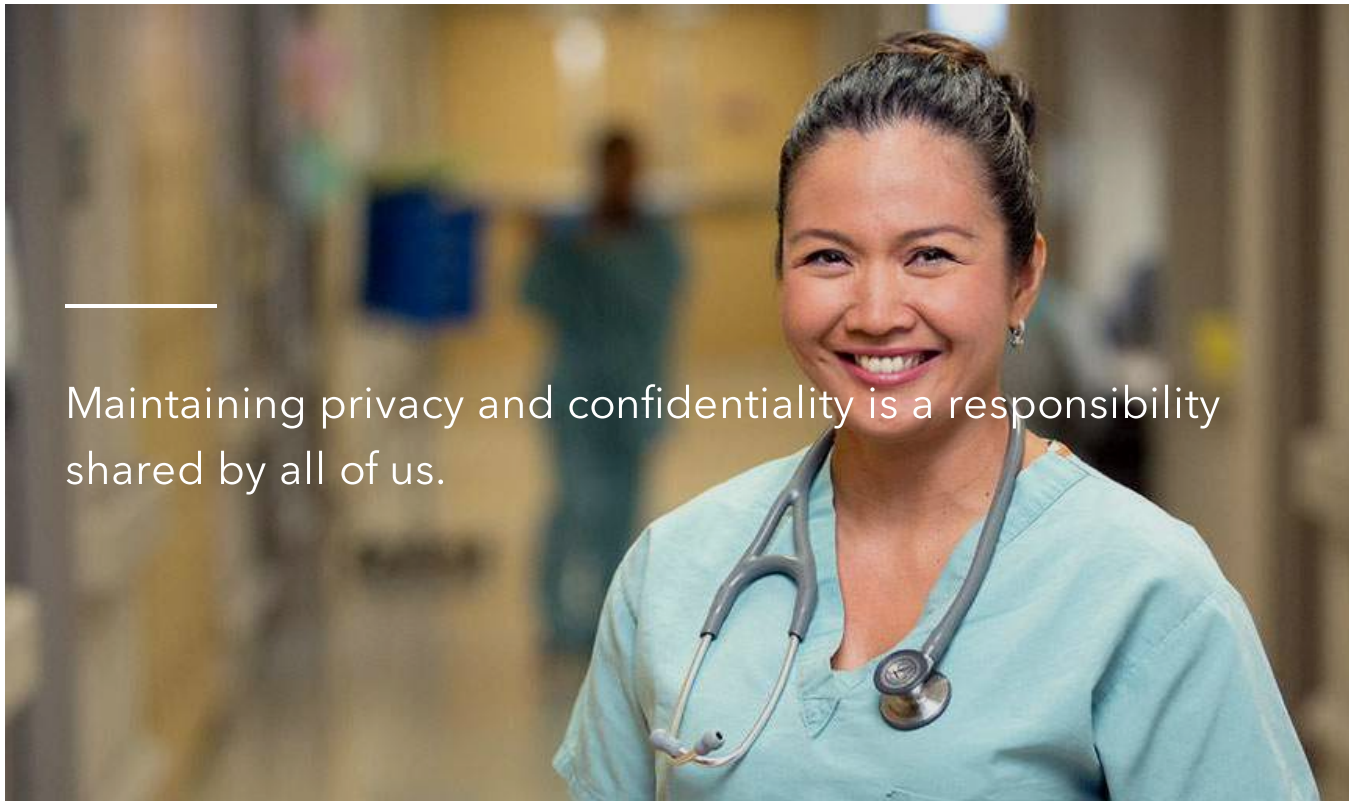
- DON'T post anything that creates or contributes to a negative or abusive environment.
- DON'T engage in Cyberbullying of any kind. Harassing, intimidating or threatening an employee, volunteer, patient or the organization in any way is unacceptable. Cyberbullying is not tolerated.
- DON'T breach confidentiality.
- DON'T reveal confidential information, anything that identifies or potentially identifies, discloses PHI or sensitive details of a patient, visitor, volunteer or staff member without their permission.
- DON'T post anything that would promote the hospital without the hospital knowing. GRH has a Communications Department who manages our social media outlets and can provide support in sharing success stories.

When it comes to social media:

If in doubt, leave it out!

NEXT LESSON

Know YOUR Responsibilities



Maintaining privacy and confidentiality is a responsibility shared by all of us.

Before sharing any information, ask yourself...

Do I have to know this information to do my job?

Access hospital information only when it **directly relates** to your job responsibilities and is necessary to perform your job. Similarly, share hospital information with individuals only when it is **necessary** to do your job.

Does anyone else have access to information, which is not necessary to do their job?

Keep hospital information secure and actively protect information from unauthorized examination or casual observation.

Remember...

“Hospital information” includes *any* information you learned while at the hospital, either verbal or written, paper or electronic.

CONTINUE

When using or sharing patient or staff personnel information, we are all expected to:

- 1 Be familiar with the Privacy Policies and their accompanying procedures
- 2 Ensure the ‘need-to-know’ principle is being met. Keep information sharing about a patient’s health information or care within the ‘circle of care’
- 3 Avoid speaking about private information in a public area

4

Consider whether you require express consent from an individual prior to collecting, using or sharing any personal information

5

Always contact staff or the Privacy Office if you have any questions about Privacy

[CONTINUE TO PRIVACY PLEDGE](#)

Privacy Pledge

Please carefully read the **Privacy, Security & Confidentiality Pledge, Acknowledgement & Agreement** (Privacy Pledge) below.

By clicking "**I agree**" at the bottom, you are acknowledging that you are aware of, understand and will comply with the terms and conditions in the GRH Privacy Pledge.

PRIVACY, SECURITY & CONFIDENTIALITY PLEDGE, ACKNOWLEDGEMENT & AGREEMENT

(Privacy Pledge)

I pledge to keep confidential any information obtained during the performance of my duties at Grand River Hospital (GRH). I understand that confidential information, meaning information that I have only because of my affiliation with GRH, includes, but is not limited to, information relating to:

Personal health information (PHI): PHIPA (s. 4) defines PHI as identifying information about an individual in oral or recorded form, if the information:

- Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family
- Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual
- Is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual

- Relates to payments or eligibility for health care in respect of the individual
- Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance
- Is the individual's health number
- Identifies an individual's substitute decision-maker

This means PHI in any format (including paper or electronic) conversations, registration information, financial history, the fact that someone is, has been or may become a patient of Grand River Hospital

Personal information (PI): FIPPA defines PI as a broad category of information, of which personal health information or PHI is one type. PI includes, but is not limited to information about any individual relating to:

- race or ethnic origin, religion,
- age, sexual orientation, or marital status.
- personal opinions or views (with some exceptions), and
- education, medical, psychiatric, criminal or employment history of the individual

This means PI of GRH employees, physicians, students, volunteers, researchers, contractors or vendors (such as but not limited to employee records, disciplinary action, performance reviews)

GRH Confidential information: includes information, in any format, created or received by the Hospital in the course of its business, executive and corporate information (including, but not limited to, information pertaining to the Hospital medical staff in their professional capacity, Board and Executive Committee meeting minutes, working drafts of corporate documents), financial information, human resources information (including, but not limited to, payroll, personnel, or legal information, and staff health records - to the extent the information is not also Personal Information).

This means information such as, but not limited to contracts, financial information, memos, peer review information, quality reports etc.

By signing this Privacy Pledge, I am acknowledging that I understand and agree to the following:

1. I am only allowed to collect, use or disclose (including: receive, look at, access, ask for, view, copy, record, print, read, listen, share with others) confidential information on a "need to know basis" only, and even then only the minimum amount required, as required for my role or as I have been authorized to do so or as required by law. If I have any doubt as to whether I am permitted to access, use or disclose confidential, I will consult my manager/supervisor or the GRH Privacy and Access Office (PAO).
2. I will not communicate confidential information either within or outside GRH, except to persons authorized to receive such information and only for the purposes of performing my duties. For clarity, I will not access, use or disclose PHI for the purpose of: training or education (including self-directed training or education) following-up on the health status of a former patient (even on compassionate grounds), including to send a note to a former patient or his/her family; providing PHI to someone in or outside of GRH requesting it for purposes unrelated to providing health care to the patient; or any work, activity or research that I am engaged in outside of GRH without written permission from my supervisor/manager or the Privacy and Access Office.
3. I will not collect, use or disclose the confidential information of family, friends, acquaintances or co-workers and will only access my own PHI by making a request through the GRH Health Records department. Unless required to perform my work at/for GRH, I am not allowed to access the PHI of any person who is a celebrity or otherwise the subject of media attention or in the public eye.
4. I will not share my passwords or credentials to GRH electronic information systems with anyone, even with an employee or affiliate or a person authorized to access the system. I understand I am responsible for protecting my passwords and access to GRH's systems and records and that I am responsible for all actions performed when the electronic information system has been opened using my password.
5. I will access, process and transmit confidential information using only authorized hardware, software, or other authorized equipment. I understand that I may not save confidential information on an unencrypted USB key or other unencrypted portable device.
6. I shall not remove confidential information from GRH premises (including taking it home to work on) except as authorized. If authorized, I shall securely store the information and ensure it

is in my custody and control at all times. PHI must not be removed from GRH in any form, on any device (laptop, tablet, memory stick, phone). I am not allowed to photograph PHI. I understand that posting or otherwise communicating PHI of anyone other than myself, on social media, chat or like electronic platforms, is an unauthorized removal and disclosure of the PHI.

7. I will not alter, destroy, copy or interfere with confidential information, except with authorization and in accordance with GRH policies and procedures.

8. I will immediately report all incidents involving loss, theft or unauthorized use or disclosure of confidential information to my immediate supervisor/manager and to GRH's Privacy and Access Office.

9. I will comply with GRH's privacy and security-related policies. If I need help understanding these policies, I will ask my supervisor/manager or contact the GRH Privacy and Access Office.

I understand that GRH audits access to its records. GRH has a right even where it does not have an obligation to disclose my name to any affected patient, his or her counsel and the Office of the Information and Privacy Commissioner if I access, use, disclose or destroy PHI for an unauthorized purpose.

I understand that by failing to comply with a term of this Privacy Pledge, I may also be failing to comply with privacy or other law, or infringing the rights of another person. A failure to comply may result in corrective action that may include but is not limited to: an investigation, retraining, loss of access to systems, reporting my conduct to a professional regulatory body or sponsoring agency, school or institution, reporting my conduct to the Information and Privacy Commissioner of Ontario, restriction or revocation of privileges prosecution, fine and/or money damages as well as action taken by GRH to limit, suspend or terminate my affiliation with GRH.

I understand and agree to abide by the conditions outlined in this pledge, and they will remain in force even if I cease to be employed by or associated with GRH.



Please read the Privacy Pledge before moving on

Thank You!

[CONTINUE TO THE FINAL QUIZ](#)

Final Quiz

You will be asked to select the most correct answer in response to a few short multiple choice questions. You will have unlimited attempts to achieve a passing score of 80% which is required before moving on.

01/05

You go to a gym every Monday and meet the same people, including a person named Sue. One Monday, Sue is not there. One of the people asks if you have seen Sue at the hospital and if so, how is she doing? How would you respond?

- a) You say you haven't seen her and suggest they try reaching out to Sue directly.

- b) You tell them Sue came in last Thursday for a minor surgery. But the surgery went very well and she is expected to be discharged soon.

02/05

You discover a volunteer colleague has been accessing information about a patient who is their neighbour. What should you do?

- a) You contact your Manager or the Privacy Office to investigate.
- b) You decide it is probably not harming the patient so you do not report it.

03/05

You go to the cafeteria to have your lunch. While walking up to a table, you notice documents that are left unattended. Upon closer look you notice these documents contain quite a bit of PI/PHI. What do you do?

- Leave the documents where you found them. You didn't lose them, so it's not your responsibility.

- Pick up the documents and contain them so it cannot be seen by others. Then take the documents to your staff contact; informing them of where and when they were found.

04/05

You receive an inquiry from someone looking for a specific patient at the hospital where you work. You look into the Patient Locator and see that they are not admitted here, but are admitted at the other hospital in Kitchener. What do you tell them?

- a) You let the individual know that we don't have anyone by that name in the hospital and nothing more (because you are not privy to their PHI).

- b) You let the individual know that we don't have anyone by that name in the hospital, but someone by that name is currently admitted at the other Kitchener hospital.

05/05

You become aware that a close friend of yours has been admitted to the hospital that you work at. You've known this person for years and are concerned for their well-being. Can you ask the nursing staff for updates on their status and treatment plan?

- Yes - the patient would probably want you to any ways.

- No - you are not part of the patient's "circle of care" and have not gotten the patient's consent.

Thank you!

Thank you for your
continued commitment to
protecting privacy!

If you have questions about privacy or security of PHI/PI, contact your manager or your hospital's Information Privacy & Security team.

- Hospital Policy & Procedures and approved forms are available on the GRH Intranet
- For general privacy inquiries - confidentiallyspeaking@grhosp.on.ca, x5305
- Information & Privacy Commissioner of Ontario - www.ipc.on.ca





You have successfully completed this e-learning course. You may now close the browser window.

Thank you!