PHIPA, FIPPA and Privacy Protection

What you will take away from this handout ..

- What are patients rights under FIPPA (Freedom of Information & Protection of Privacy Act)
- What are the protections that we provide the patients under PHIPA (Personal Health Information Protection Act)
- What are your responsibilities as a hospital employee under FIPPA & PHIPA
- What resources are available to you when you have to sort all this FIPPA & PHIPA stuff out!!!
- How are you going to protect patient / client privacy at all times.

PLEASE NOTE

This presentation is just an outline to make you aware of the basics of FIPPA, PHIPA and Privacy.

- HGH has a Privacy Officer to whom you can refer questions.
- HGH has a number of SOP and Policies that should be referred to when questions around FIPPA, PHIPA and Privacy including:
  - ADM-01-102: FIPPA
  - ADM-01-103: PHIPA
  - ADM-07-101: Management Information System
  - 12-68-129: Patient Accessibility to their Medical Records
  - 15-100-84: Responsibility of employees as to confidentiality, privacy and security of patients

Let's start with FIPPA …..

- The Freedom of Information & Protection of Privacy Act (FIPPA), is legislation that gives the public the right to request certain records of public institutions, including hospitals.
- FIPPA regulates the collection, use and disclosure of personal information, and the retention, destruction, security and accuracy of personal information; it requires hospitals to maintain certain data banks; it applies to all existing corporate records back to 2007.
- FIPPA applies to individuals who are not patients (ei: personnel, volunteers, individuals in the community) whereas the Personal Health Information Protection Act (PHIPA) applies to patients info at the hospital.

Privacy Rules related to Information Collection

- Information must be collected from the individual from whom it related unless the individual consents to the indirect collection from that specific third person.
- The information collected must be used to fulfill the purpose or function for which the hospital collect it; if it is going to be used for a different purpose the individual must give written consent.
- The information must not disclose personal information unless the disclosure is to fulfill the purpose for which the hospital originally collected it and consent has be given in writing.

Privacy Rules related to FIPPA

- Reasonable measures must be taken to protect personal information from unauthorized access, loss, theft, inadvertent destruction or alteration and damage.
- Only those individuals who need the records to perform their job have access to it.
- The information must be kept for at least 1 year after it is used unless the individual consent to earlier disposal; this retention period provides individuals with reasonable opportunity to access and correct their personal information.
- Hospitals must ensure that information is stored, transported and disposed of in a secure and confidential manner and that a record of the movement and destruction is maintained.

Freedom of Information under FIPPA

- Certain information can be requested by the public under FIPPA
- To request information the requestor must make the application in writing providing sufficient detail to locate records and indicating clearly that the request is being made under FIPPA.
- There is an application fee for obtaining the information.
- The institutions obligations must offer assistance in reformulating a request if the request is not clear.
- The institution must then conduct a reasonable search for responsive record and issue an 'access decision to the request within 30 calendar days after the request is received.

Freedom of Information Request

- If a freedom of information (FOI) request is made, it will be organized by the individual at HGH responsible for FIPPA, PHIPA and Privacy.
- You may be asked to search for information related to the request. Any of the following may be requested:
- All recorded information, however recorded, including: Drafts, post-it notes, hard drive files, email, voice mail, agendas, address books,
  - E-mails and / or correspondence
  - Expense accounts and receipts; Tenders/Bids
  - Amount of money spent on various programs
  - Briefing notes – briefing binders
  - Consultants (e.g. names, amount spent, work done)

Because the rules related to FIPPA can be complex, please ensure that all requests go to the FIPPA Coordinator.

Exclusion and exemptions from FOI Requests

Some information is excluded from FOI requests:

- Labour and employment related records
- Records relating the personal practice of a regulated health professional
- Record relating to the appointments and privileging of physicians / professionals
- Research records and teaching materials
- Legally privileged information
- Information that may impact a law enforcement case

Now ….. PHIPA

- Personal Health Information Protection Act (PHIPA) prescribes rules for the collection, use and disclosure of personal health information (PHI) in all types of health care settings, laboratories, ambulance services, nursing homes and applies to all regulated and non-regulated health care professionals.
- Under PHIPA, patients are entitled to request access to their own records of personal health information, including hospital records. PHIPA also allows a substitute decision-maker to access records of personal health information on behalf of another individual in defined circumstances

Personal Health Information

- PHIPA defines personal health information (PHI) as identifiable information relating to an individual's health and health care history. PHI includes :
  - Diagnostic, treatment and care information relating to both physical and mental health
  - OHIP numbers
  - Genetic information
  - Payments or eligibility for health care
  - Donations, testing or examination of any body part or bodily substance
  - Information identifying the patients/clients substitute decision maker
  - Other health record details
- Generally the PHI that we collect is covered by 'implied consent' ie we ask questions to collect personal health information that the patient/client answers voluntarily.
- If the information that we collect is used for any other purpose further consent is required from the patient/client.

The Difference between FIPPA & PHIPA is ……

- Personal information is different from personal health information.
- PHIPA governs personal health information (PHI).
- Generally speaking, the purpose of FIPPA is to protect the privacy of individuals and the purpose of PHIPA is to protect the privacy of individuals who receive health care.
- FIPPA applies to individuals who are not patients (ei: personnel, volunteers, individuals in the community) whereas PHIPA applies to patients at the hospital.
- Under FIPPA anyone can make a request but with PHIPA only the subject individual can make a request for PHI

Health Information Custodian (HIC) – That's You!!!

- When you are employed by any institution covered under PHIPA you become a Health Information Custodian.
- Whether you are a nurse, computer tech, radiology technician, clerk or work in medical records, you have access to health care information about the patients / clients serviced by HGH and so have the responsibility for safeguarding their privacy. Remember …. When you joined the staff of HGH you sign a confidentiality agreement to safeguard this privacy.
- The patients are entrusting you with maintaining their privacy.

Safeguarding Patient Privacy as a HIC

- **DO NOT** discuss personal health information in public places. If you have to review an individual's personal health information with them, attention should be paid to your surroundings – it is best to be cautious when communicating personal health information.
- **DO NOT** access the personal health information of individuals to whom you are not providing health care.
- **DO NOT** leave records of personal health information unattended or unsecured.
- **DO NOT** remove personal health information from a secure environment unless it is necessary and unless appropriate safeguards are implemented.
- **DO NOT** discuss patient personal information with health care providers outside the circle of care (See the PHIPA Policy for the definition of Circle of Care).
- **DO NOT** write down or share your passwords.
- **DO NOT** retain personal health information on a mobile device for longer than necessary; once the information if seen it should be deleted.
- **DO NOT** place records of personal health information in the trash or in recycling – dispose of all paper you use during the day securely in the locked paper disposal boxes .

Other Privacy Measures

- Security safeguards help to protect personal health information against loss or theft as well as unauthorized access, disclosure, copying, use or modification.
- In order to ensure that personal health information is protected, the following measures have been implemented:
  - Physical protections
  - Administrative protections
  - Technological protections

Physical Protection includes:

- Locking of cabinets /rooms where PHI is stored
- Locked offices with restricted access
- Not leaving personal health information in unsecured areas where unauthorized personnel or members of the public could access

Administrative Protection includes:

- Confirmation of identity before providing access to PHI
- Sign-out procedures for health records
- Limiting Access on a "need to know basis"
- Requirements to sign confidentiality agreements
- Policies and Procedures
- Awareness and Training

Technological Protection includes:

- Use of Firewalls and Encryption
- Strong password requirements and expectation to not share those passwords
- Access Controls
- Auditing (yes …. we can check who looked up what!!!)
- Staff must secure their computer and electronic information at all times.
- Staff are required to either lock the screen of their computer (Ctl – Alt – Del) or log-off when left unattended.
- Staff are responsible and accountable for any unauthorized access caused by leaving their computer logged-on and unattended.

Safeguarding the Security of Mobile Devices

- Security for mobile devices connected to HGH resources must be safeguarded at all time
- Never share your device with family, friends or co-workers
- If accessing PHI always ensure that you are in a private area to protect privacy of patient
- Never share your passwords
- You are accountable for all activity using HGH resources (email, network, applications)
- Protect it from loss or theft
- Report it immediately to MIS

OK …. What are the Safeguards for FAXing

- PHI should only be transmitted by FAX in urgent or emergency situations related to patient care.
- FAX's should never be sent to areas not providing patient care such as insurance companies and lawyers offices.
- Verify that you have the right FAX number … any questions about the number call the recipient to double check it is the right number.
- Verify the FAX number and dial with care, confirm the number visually before pressing 'Send'.
- Use discrimination in sending only documents that are required to deliver care to the patient.

Safeguards when Using Email / Smart Phones

A physician is asking me send some information about the patient via email …. Can I do it?

- PHI can only be sent via the HGH Email (this will encrypt the contents making it private) where the recipient has a "need to know" the information and the following precautions are:
  - Use "Private" and "Confidential" flags to alert the recipient that the message contains PHI
  - Do not include PHI in the subject
  - Verify all "To" fields before sending message making sure it is only being sent to MD
  - All electronic communications relating to treatments shall be printed and stored in the patient chart.
  - The information needs to be deleted from the device as soon as it is seen and printed.

The Police called … what can I tell them?

- With limited exceptions, employees may not disclose patient information to the police. All police requests for personal health information about a patient should be redirected towards Medical Records.
- Outside of regular hours the administrator on call should be notified.
- There are only 3 ways for the police to obtain information about a patient outside of a courtroom
  - The patient provides consent
  - The police present a search warrant
  - As required by specific law …..
- If a patient is treated fro a gunshot wound, a person has a duty to notify police of certain situations even where this means disclosing PHI without consent or warrant. This disclosure must be made orally and as soon as is reasonably practical to do so, without interfering with the person's treatment or disrupting regular HGH activities (SOP 14-82-86).
- If an employee believes, on reasonable grounds, that the disclosure is necessary for the purpose of eliminating a significant risk of serious bodily harm to a person or group of persons (for example the patient is being discharged and is threatening to harm a person in the community. Administrator on duty should be consulted prior to this disclosure.

Telephone Inquiries

The patients clergy is calling to see how the patient is … what can I tell them?

- Over the phone the rules of privacy are the same for all callers … family, friends and clergy.
- PHIPA allow for disclosure of basic information only over the telephone unless the patient has requested no information be provided:
- Basic information means:
  - That the person is a patient in the hospital
  - The location of the patient in the hospital
  - The patients general health status (critical, poor, stable or satisfactory)

PLEASE NOTE …. Mandatory Disclosures

- PHIPA specifically permits the disclose of PHI for a number of purposes required statutes. The PHIPA Policy (ADM-01-103) Attachment 3 clearly outlines those mandatory disclosures and the Acts that authorize the disclosure so please refer to the policy when disclosure is being considered . Some example of the mandatory disclosures that may affect you if you are in a clinical area include:
  - Disclosure to the Children's Aid Society in the case of Child Abuse
  - Disclosure to the Chief Medical Officer in the case of a communicable disease outbreak
  - Disclosure to the Coroner about the facts surrounding the some deaths (See ADM-01-103: Attachment 3 for explanation)

Privacy Breaches

A privacy breach is the unauthorized access, collection, use or disclosure of PHI.

- It may be intentional: purposely accessing the PHI of your neighbour when you do not require such information to do your job
- It may be inadvertent: accidental sending a medical report on a patient to the wrong fax number
- It may due to failure to protect PHI: leaving health records unattended or sharing passwords
- It includes any lost or stolen PHI

Example of Intentional Privacy Breach

- You hear that a neighbour has been admitted to HGH.
- You want to find out why they have been admitted so you look their records up on the computer.
- This is a privacy breach and is cause for disciplinary action up to and including dismissal or termination of hospital privileges.
- There is also a significant fine ($25,000) that will be levied against the individual who breaches PHIPA rules
- In addition, privacy breaches involving regulated health professionals will be reported to their respective college.

Intentional Privacy Breach: Social Media

- Personal health information should never be discussed on social media, such as Facebook, Twitter, etc. (even as a personal message)
- Remember personal health information includes any identifying information about an individual in oral or recorded form.
- Even if you believe it to be harmless, the smallest details can reveal personal health information.
- For example, even without disclosing the patient's name, if you provide a patient's age, condition, where you work in the hospital, the circumstances leading the hospitalization, then that individual could be identified and you have breached their privacy.

- **Remember that a privacy breach means the unauthorized access, collection, use, disclosure or disposal of any personal health information and personal information.**
- **Purposely accessing information you do not require to do your job, even if intentions are good, is a breach of privacy.**
- **Audits are conducted on the hospital's electronic records for this purpose.**
- **Remember that sharing any information about the patients that you care for outside of their 'circle of care' is also considered a privacy breach.**

Example of Unintentional Privacy Breach

- You suddenly realize that you have put the wrong number into the FAX machine so that confidential information has been sent accidentally to an unauthorized recipient over a FAX.
- You must immediately contact the recipient of the faxed information and request that they destroy the material in a secure and confidential manner.
- You must notify your Manager as well as the Privacy Officer with details of the breach, the specifics of the PHI at issue as well as the steps taken to ensure this does not happen again.

Example of Failure to Protect PHI

- You are asked to photocopy or print out part of the patient's chart.
- You decide to a have a chat with someone down the hall while it is printing.
- Someone walking past the photocopier / printer picks up the chart and walks away with it so they can use the identifiers for criminal intent (fake health cards or social security number cards)
- This would be a failure to protect PHI and a privacy breach.
- You must notify your Manager as well as the Privacy Officer with details of the breach and the specifics of the PHI at issue

'Take Aways' from this Presentation

- **As a member of HGH staff you are responsible for keeping patient health information private and safe.**
- **There is legislation in place to safeguard information in the hospital and the precepts of that legislation is included in the HGH polices related to privacy, FIPPA and PHIPA.**
- **When questions arise related to privacy, FIPPA and PHIPA find the policies to help guide you through the issue.**
- **HGH has a Privacy Officer to also help guide you. If the question arises after normal business hours, refer questions to the Admin on call.**