Module 5 – Privacy and Security of Health Information

This unit is designed to provide the participant with information on the concepts of confidentiality, privacy and security, related to dealing with patients and their personal health information.

Participants are to be cognizant of the fact that one of the founding concepts of Health Information Management Professionals, is to uphold and make secure the confidential health information of patients at all times.

Participants accessing this module must be aware that the information presented is very high level, and of the fact that they should contact their local governmental legislated bodies, to obtain specific regional information that may exist, governing patient privacy and the access to health records.

OBJECTIVES:

At the conclusion of this unit, the participant should be able to:

1. Define the terms of Confidentiality, Privacy, Personal Health Information and Security.
2. Define what constitutes Confidential Information.
3. Understand the concepts of right to access of the health record.
4. Describe the right of patients to consent to use and disclosure
5. Understand the existence of legislation, governing same.
6. Define the 10 universal privacy principles, guiding legislation.
7. Be familiar with the strategies to manage privacy in a health care setting, for paper and electronic documents.
8. Be able to apply concepts presented to manage the maintenance, protection and disclosure of patient information.

A. Key Definitions:

i) Patient Confidentiality:

Whereby the health information that is confided by a patient, family member or guardian, is kept secret and not disclosed or made accessible to others unless authorized by the consent of the patient or as authorized by law.

ii) Privacy:

Refers to the right of individuals, groups of individuals or organizations to determine for themselves, when, how and to what extent, information about them is communicated to others.

With respect to health information, the right of privacy includes a patient's right to know of and exercise control over any information about him or her. It includes a right to informed consent.

iii) Personal Health Information:

Is defined as information about an individual, that relates to the physical or mental health of the person. This can include more than just the paper or electronic health record, and also includes videos, photos, audio files, tracings, and any other media where health information is collected or stored.

iv) Security:

The state of being free from danger or threat.

In relation to the protection of personal health information, this refers to the need to implement reasonable physical, technical and administrative measures to safeguard patient information.

B. What Constitutes Confidential Information?

Confidential information includes any patient information, and goes beyond the traditional health record. It also includes any conversations about the patient, or their financial or family situations.

In most jurisdictions, privacy legislation also includes mention of confidential information within the work place. This includes information about your co-workers, including their employment records, salaries, and any personal or family circumstances. It is also considered to include business information about your employer. For example, if you are employed by a hospital, it would include internal reports, strategic planning documents, statistical and financial records.

C. Rights to Access of the Health Record, and Patient Consent

Implied Consent = permits one to conclude from surrounding circumstances that a patient would reasonably agree to the collection, use or disclosure of the patient's personal health information.

Express Consent = is obtained when patients explicitly agree to the collection, use or disclosure of their health record.

Generally, an organization must have either express (verbal or signed consent) or implied consent (implied by virtue of the patient arriving and requesting treatment) in order to collect, use or disclose information. Many nations rely on the implied consent model. The Implied Consent model permits care providers to share clinical records with others involved in providing treatment, such as physicians, nursing personnel, consultants, and other members of the clinical team – without the signed or express consent of the patient.

For example, if a patient arrives in an Emergency Department with chest pain, and must be transferred to another hospital to undergo a Cardiac Catheterization, by virtue of the patient's arrival for treatment and discussion with the treating physician, if the patient agrees to be transferred to the other facility, the Emergency Department physician can forward clinical notes to the accepting physician, without actually obtaining consent to do so directly from the patient.

Express Consent is required if you are disclosing personal health information for a purpose other than for the provision of health care. Such examples of this would be to an insurance company, an employer, etc. Basically, any request that is not directly related to the immediate or ongoing care of the patient. In such cases, it is recommended to obtain the signed, dated and witnessed consent of the patient.

Guidelines for Obtaining Consent

- To be a valid consent, the patient must have the capacity to consent. If the patient does not have the capacity, you must obtain the consent from the patient's Substitute Decision Maker (SDM). In most cases, this is the parent or next-of-kin of the patient.

- Just as patients have the right to consent, they must also have the right to withdraw consent at any time. For example, a patient may consent to releasing their health records to a Researcher, and some time later contact the organization holding their records, and state they no longer wish their records to be shared. In such cases, it is recommended to obtain a signed "withdrawal of consent" from the patient, in order to avoid any future confusion.

To Be a Valid Consent:

a) The patient must have the capacity to consent

b) The consent must be obtained directly form the patient or their SDM (if applicable)

c) The consent must be related only to the information in question

d) It must be obtained voluntarily without deception or coercion

e) It must be reasonable to believe that the patient understands why you are disclosing the information and that they have the right to withdraw consent.

Patient Capacity

This can be a sensitive area, and local legislation should be reviewed to determine if there are guidelines available indicating how to deal with the capacity of a patient having the ability to consent to releasing their information.

In order to be deemed incapable to consent, it is generally accepted that such a determination must be made, and documented within the patient health record, by a qualified healthcare provider. It should also be noted that a patient's ability to consent may change over time, depending on their condition, and that you must consider the patient's capacity each time you seek consent.

When a patient is considered unable to consent, there is a generally accepted hierarchy of substitute decision makers, who would consent on behalf of the patient:

- Guardian
- Power of Attorney for Personal Care
- Spouse or partner
- Child, custodial parent
- Brother or sister
- Other relative

If a patient is deceased, then consent to releasing information falls to the Executor of the Estate. If the patient expired without indicating an Executor, then it would fall to the individual who is in charge of administering the patient's estate, and acting in this capacity.

Consent Involving Children and Teenagers

This too can be a sensitive area, and please refer to local legislation concerning capacity for consent, for children and adolescents.

I shall reference Canadian Law as an example in this regard.

If the healthcare provider involved in the care and the treatment of the child deems they understand what they are consenting to, and have the mental capacity to do so – then the child – regardless of age – has the right to consent. If not, it is generally accepted that a parent/guardian can consent on their behalf up to the age of 16. After that age, consent will be obtained from the patient (unless they have a medical condition that renders them below the mental capacity of a healthy 16 year old).

If there is a conflict between releasing information of a capable child and a parent/guardian, the capable child's decision prevails over that of their parent/guardian.

D. Privacy Principles:

As indicated earlier, when dealing with personal health information, most legislation, regulatory guidelines, ethics and policies, follow the 10 principles listed below. You may also see them referred to as the 10 Fair Information Principles.

1. Accountability
2. Identifying purposes for collection of personal information
3. Consent for the collection, use and disclosure of personal information
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

There may be slight variations of this listing within your nation, and for the purposes of this Learning Module, we shall be referencing those used in Canada, under the Canadian Standards Association's Model for Code for the Protection of Personal Information.

1) Accountability

"An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles."

How is this principle applied?
Health care facilities are required to implement organizational policies and procedures to protect Personal Health Information (PHI). This includes the designation of a person responsible for privacy obligations, to address access requests, privacy related inquiries and complaints, and assist in any external privacy investigations. This person is usually known as the Privacy Officer. All employees, physicians and volunteers having access to PHI are considered accountable.

2) Identifying Purposes

"The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected."

How is this principle applied?
Patients are to be informed of the purposes for which their PHI is collected, used, and disclosed. It is common practice to display a statement in public places, such as a registration area, that advises that information is collected for the provision of health care and may be shared with other care providers. This statement should

include a general description of the organization's privacy practices, how to contact the Privacy Officer, how to obtain access to records or lodge a concern, and how to limit access.

3) Consent

"The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. **Note:** *In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information."*

How is this principle applied?
This was one of the most challenging principles to operationalize in the health setting, because information must be collected by a health care provider to provide care; it must be disclosed to others in the provision of care (e.g., pharmacists, specialists); and it must be used by yet others to process claims and manage the hospital or health system. Jurisdictional health information legislation generally permits the collection of personal information on the basis of a knowledgeable, implied consent model, deemed consent model, or no consent for the collection of information. In terms of use and disclosure of the information, jurisdictional health information statutes generally specify permissible uses and disclosures as well as whether or not further consent is required for the use or disclosure (e.g., fundraising or research). The statutes may also offer the individual the option of requesting that their information be masked or not further disclosed.

This is a complex area of health information management. The HIM professional should study the consent provisions set out in their jurisdiction and be fully familiar with the model their jurisdiction has adopted as well as the details of the consent management solutions in their e-health systems.

4) Limiting Collection

"The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means."

How is the principle applied?
Data that is not required for the delivery of health care or associated administrative functions should not be collected. There must always be a reason to collect any data element, and facilities must guard against collection of data that "may be useful"

someday. This principle makes that point that you can only ask questions of your patients that are required in order for you to perform your duties.

5) Limiting Use, Disclosure, and Retention

"Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes."

How is the principle applied?
Unless otherwise explained and consented to, PHI should not be shared or retained longer than is required to fulfil the functions. It is recognized that there are occasions when this principle is overruled by law, (e.g., receipt of a subpoena or Coroner's Warrant; or for reporting of suspected elder or child abuse). Various legislation and professional regulations will specify the minimum requirement for certain documentation.

6) Accuracy

"Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."

How is the principle applied?
Health care delivery depends on accurate and timely data. It is incumbent upon an organization to have policies and procedures in place to measure and evaluate the accuracy and timeliness of PHI in order to provide the best possible care. This principle reiterates the importance of collecting information accurately, and includes information as basic as the patient's name, date of birth, family physician, home address, and any health insurance information. An error at the beginning of the patient's encounter at the time of registration, will feed through to all other systems within the organization.

7) Safeguards

"Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."

How is the principle applied?
Organizations must implement appropriate technical, administrative, and physical safeguards to protect PHI. A component of this is to ensure all employees, volunteers, and anyone else exposed to PHI are well informed of their responsibilities related to privacy and confidentiality. Organizations are responsible for implementing comprehensive privacy policies which should include education at the time of hire/arrival, with regular reviews for employees, physicians, and volunteers. Best practice includes the creation of a privacy training program for the organization which would include the signing of an Oath of Confidentiality by all who have access to PHI.

All training and the Oath of Confidentiality should clearly state that under no circumstances is any staff member to access the health record of an individual,

unless doing so is a requirement of their employment. Snooping is not to be tolerated.

Ensuring Safeguards

"Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."

Protecting PHI is challenging particularly in an electronic multi-jurisdictional environment. Key to meeting this principle is the development, implementation, and maintenance of technical, administrative, and physical safeguards. Technical safeguards include access controls and audits. Access controls identify authorized users and their permissions; that is, who can access what data (i.e., role based access) and at what level (e.g., create, edit, view only). This can be challenging as individuals may function in similar roles but with different access rights. For example, does an Emergency Department registration clerk have access to demographics only, or demographics and visit history? The access by role and user needs to be compared to similar roles in other facilities. The technology must include significant auditing capability (e.g., reviewing who has accessed what and when) to ensure that privacy and security are safeguarded, along with the integrity of the information.

Administrative safeguards would include establishing common policies and procedures on data privacy, security, access, and disclosure; staff training; assigning privacy responsibility to a key individual or a team; privacy provisions in vendor or contract staff contracts; and establishing rigorous standards for auditing privacy and security within the HIE. All components of these safeguards must outline the responsibilities and consequences for access, disclosure, and protection of PHI. A strong common policy and procedure on dealing with incidents and breaches must be implemented and enforced.

Physical safeguards include the core activities for computer operations. In addition to passwords (e.g., that must be unique, protected, and changed on a regular basis), physical safeguards include hardware security; redundancy, and location of back-up data; restriction on printer availability; limiting the number and location of devices with downloading capabilities (e.g., CD writers); wearing identification badges; and the safe storage and destruction of records. Safeguards also include simple practices such as locking doors to file and server areas and shielding computer monitors from the general public.

8) Openness

"An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."

How is the principle applied?
Organizations are responsible for the development of policies and a written statement on their information practices, and to display the same for patients. Best practice is to have such information posted on the facility's website and in key public areas. It should include details on how to contact the organization's Privacy Officer.

9) Access

“Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.”

How is the principle applied?
Organizations are required to grant access by an individual to their own PHI upon request, under most circumstances. Though it is rare to deny an individual access to view their own health information, there are two circumstances in which access can and should be denied: 1) if there is a threat of harm to themselves, or 2) if there is a threat of harm to others. Regional legislation covers such instances and outlines the right to appeal to the provincial, state, territorial Privacy Commissioner in cases where denial has occurred.

The right to amend PHI means that an individual can challenge the accuracy and completeness of their information and request that an amendment be affixed to any document clearly outlining the area of contention. An amendment is a document, written, signed, and dated by the person indicating what information they believe is inaccurate or incomplete. As a legal document, the health record (whether paper or electronic) cannot be altered or destroyed**;** however**,** an addendum can be added as a permanent part of the clinical documentation. Anyone sent a copy of the original documentation must be sent a copy of the addendum, as it is the right of the patient and responsibility of the facility to ensure that all in possession of the original document are made aware of the addendum. Due to the right of an individual to request an amendment to their information, a log or tracking tool is necessary so that it is clear who has accessed information, for what purpose, and when it was disclosed. Any amendments can then be sent to those who have a copy or access to the original information.

If an organization becomes aware of a breach of privacy where PHI is accessed, it is best practice (and in some jurisdictions, the law) to inform the individual immediately of the breach. The organizations’ policies and procedures will reflect the process of when this is to be completed, how this is to be done, by whom, and under what circumstances.

10) Challenging Compliance

“An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance”

How is the principle applied?
Each facility or organization holding PHI must develop a compliance policy and procedure detailing the process for individuals or their representatives to challenge the facility’s privacy practices. Such challenges would be referred to the organization’s Privacy Officer. Best practice is to have the procedure posted prominently in the facility (e.g., on the facility’s website or in areas easily accessible by the public).

E. Security of Patient Information:

1) Security Policies

Each organization must have processes in place to keep personal health information secure. How this is undertaken may vary depending on the organization's size and complexity. At the very least, each organization should have a Security Policy that details the organization's commitment to appropriate security measures, and provides high level details on strategies in place to make it happen.

Security breaches can range from not locking doors to file rooms, entering the wrong fax number when sending patient reports, leaving patient information lying around, sharing your passwords with someone else, etc.

A security policy is important as a guidance document to all levels of staff within your organization, and will assist them in creating their own departmental level standards and procedures. As Health Information Management Professionals, we have ethical obligations, in addition to regional legal and regulatory obligations, to protect patient information. Many of the security concepts overlap between the HIM and Computer Information Services departments, and the two traditionally work closely to monitor and deal with security of PHI related software concerns.

Points to Consider Including Within a Security Policy

- What security means to your organization, and why it is important
- Your guiding security goals and principles
- Basic security and accountability responsibilities of all personnel, physicians and volunteers
- A regular (recommended at hire and once a year thereafter) Privacy and Security Training Program for all personnel, physicians and volunteers
- Identify an individual responsible to regularly review and update the policy, if needed
- How to protect access to patient information (in the case of electronic health records, documented rules related to access levels and password rules)
- Physical measures in place to control access and ensure security of PHI.
- How to deal with external vendors and contractors, providing software support, etc, that may require access to PHI.
- A Confidentiality Agreement that must be signed at time of hire.

- Appointment of an individual responsible for Privacy/Security of patient information (for example a Privacy Officer)

2) Security and People

Security is only as strong as the personnel using it. Even the best security technology can be vulnerable if you do not have staff committed to safeguarding confidential patient information. Below are some suggested steps to take in coping with the people aspect of security.

- **Inform**, educate and motivate personnel.

  Give them the required tools to carry out their personal security responsibilities. This includes training that stresses the security policy, responsibilities for physical security, rules for using fax machines, password policy (never sharing passwords), how to report incidents of breaches or near miss breaches.

  Run appropriate background checks before hiring personnel who deal with PHI, work in the Information Services environment or have special security responsibilities.

  Ensure everyone signs and understands the organization's Confidentiality Agreement.

  Gold Standard is to have privacy training at the time of hire, and once a year thereafter as part of an annual training program. Annual training programs also include training on other important issues, such as Fire Training.

- **Impose** controls to ensure nobody gains access to personal health information without proper authorization.

  This can be done by following the steps detailed in the step above, as well as working to create an organizational policy and applying rules as to what employee category should be granted to what level of computer access. For example – A billing clerk should not be able to read the operative note of a patient, contained with the electronic health record. A physician should be granted access to all electronic patient records of patients they are treating.

  Any third party vendors, contractors, etc, must sign a Confidentiality Agreement prior to having access to any sensitive PHI or organizational information.

3) Physical Security

- All personnel must be aware of

Physical security responsibilities. Locking doors, not permitting access to areas containing confidential information.

Never sharing passwords.

Signing out of a computer when they are not using same.

How to lock up sensitive information.

Always wear their organizational name badge, preferably containing a photograph, indicating they are permitted access to a secure area.

How to deal with transporting PHI outside of their immediate work environment.

Who to report to and how to report any breaches or suspected breaches or security incidents.

How to dispose of paper copy PHI (ie. shredding systems in place)

- Work with the Information Systems Department to ensure

  All computers must require passwords to access.

  Ensure computer monitors have screen savers that have "time out" capabilities, when not accessed for a period of time.

  Educate all staff on not sending PHI externally via email.

  Ensure monitors are positioned so that others cannot "read over your shoulder"

F. Privacy Breaches:

A privacy breach in a health care setting can be very serious. Some regions have financial penalties built into their legislation, in dealing with malicious and intentional breaches involved patient personal health information. A breach can range from a misdirected fax to a theft of a laptop, snooping at the health record of an individual you are not involved in the care or treatment of, or the selling of patient information to a marketing firm.

Each organization should create a "Breach Management Policy", which details steps to take when investigating a breach, in order to produce a concise investigative report. The Human Resources/Personnel Department of the organization should include a "Discipline Policy", which details how to deal with breaches, based on the seriousness and intent of the breach. Health care organizations should have a policy of termination of employment for serious, intentional and malicious breaching of patient information.

SUMMARY

In this unit, we explored the role of Health Information Management Professionals, who are responsible for the safeguarding of patient sensitive clinical information, and as such, must be aware of and involved with a myriad of related privacy and security issues throughout their professional life. In many cases, they are responsible for the oversight of privacy and security within their organizations.

It is recognized that Health Information Management Professionals are experts in their knowledge and application of regulatory, policy and information standards related to privacy and confidentiality, which are the foundation for secure personal health information. HIM's have an ethical Code of Conduct, which enshrines the professional obligation to uphold and maintain PHI at all times.

This unit provided a high level oversight of privacy and security requirements, that can be applied to any health care setting.

REVIEW QUESTIONS

1. If you are a HIM Coder, and notice your neighbour has been brought into the Emergency Department, is it OK for you to look at your neighbour's patient chart?

2. Is it permissible to sell the names of patients to someone marketing services to patients? For Example, baby formula to new moms?

3. A famous athlete is admitted to your hospital, you get a call from the local newspaper asking what their condition is. Is it OK for you to speak to the newspaper and provide them information?

4. Is it appropriate to discuss patients in public areas? In elevators, hallways?

5. A fellow employee asks you for your password to sign in and check a patient's electronic health record. Should you share this information with them?

6. Is it OK to leave the door to the File Room unlocked?

7. How many universal privacy principles are there?

8. The husband of a patient arrives in the Health Information Management Department, and is requesting a copy of the health records related to his wife. He wants to sign on her behalf and obtain the records. Is this permissible?

REFERENCES:

1. Canadian Standards Association (CSA). Privacy Code, CSA Standard CAN/CSA-Q830, *Model Code for the Protection of Personal Information.* March 1996. http://www.csa.ca/cm/ca/en/privacy-code (March 2018)

2. Canadian Health Information Management Association. *Fundamentals of Health Information Management, 2nd Edition.* Ottawa, Ontario: Canadian Healthcare Association, 2013

3. Ontario Hospital Association, Ontario Hospital eHealth Council, Ontario Medical Association, Office of the Information and Privacy Commissioner/Ontario. *Hospital Privacy Toolkit.* Ottawa, Ontario: Queen's Printer for Ontario, 2004.

4. MacDonald, Marci. Halton Healthcare eLearning Module *Privacy and Security.* Oakville, Ontario: 2017.

5. Information and Privacy Commissioner, Ontario Canada. Toronto: ON. http://www.ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=885 (March 2018)

Acknowledgement

IFHIMA would like to gratefully thank the following individual who contributed their time and efforts towards the completion of this Learning Module.

Marci MacDonald, CHIM Canada