Module 5 – Privacy and Security of Health Information

This unit is designed to provide participants with information on the concepts of confidentiality, privacy, and security as they relate to patients and their personal health information.

Proper management and control of health information are essential to maintaining trust in healthcare systems, preventing discrimination, and protecting individuals from the misuse of their personal health information.

Participants should understand that one of the foundational principles of Health Information Management (HIM) professionals is to always uphold and safeguard the confidentiality of patient health information.

Those accessing this module should note that the information presented is high-level and are encouraged to contact their local governmental and legislative bodies for specific regional regulations governing patient privacy and access to health records.

I. Objectives:

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

- Define and understand the terms confidentiality, privacy, personal health information, and security.
- Define the 10 universal privacy principles.
- Demonstrate awareness of national and international legal and regulatory compliance.
- Understand patient rights regarding access to their health information, including:
    - Consent
    - Access
    - Amendment

- Develop key strategies to manage privacy in a healthcare setting.
- Review data protection and security measures.
- Understand emerging threats and cybersecurity.
- Review risk management and breach response in a healthcare setting.
- Apply the concepts presented to manage the maintenance, protection, and disclosure of patient information.

II. Key Definitions

- Patient Confidentiality: Health information that is shared by a patient, family member, or guardian is to be kept private and not disclosed or made accessible to others unless authorized by the patient's consent or as permitted by law.
- Privacy: Refers to the right of individuals, groups, or organizations to determine when, how, and to what extent information about them is communicated to others. With respect to health information, this includes a patient's right to know and exercise control over information about themselves, including the right to informed consent.
- Personal Health Information: Information about an individual that relates to their physical or mental health. This includes not only paper or electronic health records but also videos, photos, audio files, tracings, and any other media where health information is collected or stored.
- Security: The state of being free from danger or threat. In relation to health information, this refers to implementing reasonable physical, technical, and administrative safeguards to protect patient information.

III. What Constitutes Confidential Information

Confidential information includes any patient information and extends beyond the traditional health record. It includes any discussions about a patient or their financial or family circumstances.

Privacy legislation in most jurisdictions also includes workplace confidentiality, covering information about co-workers (e.g., employment records, salaries, or family situations) and business information about the employer, such as internal reports, planning documents, or financial data.

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

Implied Consent allows one to conclude from circumstances that a patient would reasonably agree to the collection, use, or disclosure of their personal health information.

Express Consent is obtained when a patient explicitly agrees to the collection, use, or disclosure of their health record.

Organizations generally must have either express (verbal or written) or implied consent (by virtue of seeking treatment) to collect, use, or disclose information. The implied consent model allows providers to share clinical records with other members of the care team such as physicians, nurses, and consultants without requiring signed consent.

For example, if a patient arrives in the Emergency Department with chest pain and must be transferred to another hospital for a cardiac catheterization, the Emergency Department physician may forward clinical notes to the accepting physician without obtaining express consent.

Express consent is required for disclosures unrelated to care (e.g., to insurance companies or employers). In such cases, signed, dated, and witnessed consent must be obtained.

A. Guidelines for Obtaining Consent

i) For consent to be valid, the patient must have the capacity to provide it. If the patient lacks capacity, consent must be obtained from the patient's Substitute Decision Maker (SDM). In most cases, the SDM is the parent or next of kin.

ii) Just as patients have the right to provide consent, they also retain the right to withdraw it at any time. For example, a patient may initially authorize the release of their health records to a researcher but later decide to revoke that permission. In such cases, it is recommended that the organization obtain a signed "Withdrawal of Consent" form from the patient to ensure clarity and prevent future misunderstandings.

- To Be a Valid Consent:
- The patient must have the capacity to consent.

- Consent must be obtained directly from the patient or their Substitute Decision Maker (SDM).
- Consent must relate only to the information in question.
- Consent must be given voluntarily, without deception or coercion.
- It must be reasonable to believe that the patient understands why the information is being disclosed and that they may withdraw consent at any time.

iii) Patient Capacity

Determining a patient's capacity to consent should follow local legislation. Generally, a qualified healthcare provider must document a finding of incapacity in the health record. Capacity can change over time depending on the patient's condition, so it should be reassessed with each consent.

iv) When a patient cannot consent, the hierarchy of SDMs usually includes:

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

If a patient is deceased, consent to release information falls to the Executor of the Estate. If no Executor has been designated, the responsibility is transferred to the individual authorized to administer the patient's estate and act in that capacity.

B. Consent Involving Children and Teenagers

This can be a sensitive area, and it is important to refer to local legislation regarding consent capacity for children and adolescents.

As an example, under Canadian law, if the healthcare provider responsible for the child's care determines that the child understands what they are consenting to and possesses the mental capacity to do so, then the child, regardless of age, has the right to provide consent. If the child is not deemed capable, it is generally accepted that a parent or guardian may consent on their behalf up to the age of 16. After that age, consent is typically obtained directly from the patient, unless a medical condition impairs their decision-making capacity below that of a healthy 16-year-old.

In cases where a capable child and a parent or guardian disagree about the release of information, the decision of the capable child takes precedence.

V. Privacy Principles

As noted earlier, when managing personal health information, most legislation, regulatory guidelines, ethical frameworks, and organizational policies adhere to ten key principles, commonly referred to as the Ten Fair Information Principles.

- Accountability
- Identifying purposes for collection of personal information
- Consent for the collection, use and disclosure of personal information
- Limiting collection
- Limiting use, disclosure, and retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance

There may be slight variations of these principles among different countries; however, for the purposes of this learning module, we will reference the version established by the Canadian Standards Association's Model Code for the Protection of Personal Information.

i) 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 safeguard Personal Health Information (PHI). This includes designating an individual responsible for overseeing privacy obligations, managing access requests, responding to privacy-related inquiries and complaints, and assisting with external privacy investigations. This individual is typically referred to as the Privacy Officer. All employees, physicians, and volunteers who have access to PHI share accountability for maintaining its confidentiality and security.

ii) 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 must be informed of the purposes for which their Personal Health Information (PHI) is collected, used, and disclosed. It is standard practice for organizations to display a notice in public areas, such as registration desks, indicating that information is collected for the provision of health care and may be shared with other authorized care providers. This notice should include a general overview of the organization's privacy practices, instructions on how to contact the Privacy Officer, guidance on how to request access to health records or file a concern, and information on how to restrict access to their information if desired.

iii) 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?

Implementing this principle within the healthcare environment can be particularly challenging. Health care providers must collect information to deliver care, disclose it to others involved in treatment (e.g., pharmacists or specialists), and allow additional use by administrative departments for functions such as claims processing and system management.

Most jurisdictions permit the collection of personal information under one of several models: knowledgeable implied consent, deemed consent, or, in some cases, no consent for specific types of collection. Regarding the use and disclosure of information, health information legislation typically defines permissible purposes and indicates whether additional consent is required (for example, for research or fundraising). Some statutes also give individuals the right to request that their information be masked or excluded from further disclosure.

This remains a complex area of Health Information Management. HIM professionals must be thoroughly familiar with the consent provisions within their jurisdiction, understand the consent model adopted, and have a working knowledge of how consent management is implemented within their electronic health systems.

iv) 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 necessary for the delivery of health care or related administrative functions should not be collected. Each data element must have a clear and justifiable purpose, and organizations must avoid

gathering information simply because it “may be useful” in the future. This principle reinforces that only information directly relevant to providing care or fulfilling professional responsibilities should be requested from patients.

v) 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 explicitly consented to, Personal Health Information (PHI) should not be shared or retained longer than necessary to fulfill its intended purpose. However, there are circumstances in which this principle may be overridden by law. For example, in response to a subpoena, a Coroner’s Warrant, or mandatory reporting requirements such as suspected child or elder abuse. Applicable legislation and professional regulations establish the minimum retention periods for specific types of documentation.

vi) 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?

Personal Health Information (PHI) must be accurate, complete, and up to date to ensure it serves its intended purpose. Accurate and timely data are essential for the safe and effective delivery of health care. Organizations must establish policies and procedures to regularly assess and verify the accuracy of PHI.

This principle underscores the importance of collecting correct information from the outset, such as the patient’s name, date of birth, address, family physician, and insurance details. Errors made during registration or data entry can propagate throughout all connected

systems within the organization, potentially impacting patient care and administrative processes.

vii) Safeguards

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

How is the principle applied?

Protecting Personal Health Information (PHI) is increasingly complex in today’s electronic and multi-jurisdictional healthcare environment. To meet this principle, organizations must establish, implement, and maintain comprehensive technical, administrative, and physical safeguards.

Technical safeguards include access controls and audit mechanisms. Access controls define who is authorized to view or modify information and to what extent; commonly referred to as role-based access. For example, an Emergency Department registration clerk may only have access to demographic and visit information, while a treating physician may have full access to the patient’s clinical record. Robust audit capabilities are also essential to monitor who has accessed PHI, when, and for what purpose, ensuring both privacy and data integrity.

Administrative safeguards involve developing and enforcing policies and procedures governing privacy, data access, and disclosure. These measures include staff training, designating a privacy or security officer, integrating privacy clauses in vendor contracts, and conducting regular internal audits. Clear accountability and defined consequences for violations must also be established.

Physical safeguards encompass measures that protect the physical environment in which data is stored or accessed. These include secure hardware management, restricted access to file and server rooms, use of identification badges, secure printer and device placement, password-protected systems, and appropriate destruction of records. Even simple actions such as locking doors and positioning computer monitors to prevent unauthorized viewing are critical to maintaining confidentiality.

viii)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 must be transparent about their policies and practices for managing Personal Health Information (PHI). This includes developing clear, accessible documentation that outlines how PHI is collected, used, disclosed, and protected. Best practice is to make this information readily available to patients and the public, both online and in key areas within the facility, such as registration desks or waiting rooms. The posted statement should explain the organization’s commitment to privacy, summarize relevant policies, and provide contact information for the Privacy Officer. This openness fosters trust and help patients understand their rights regarding their personal health information.

ix) 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 generally required to provide individuals with access to their own Personal Health Information (PHI) upon request. Although it is uncommon to deny an individual access to their records, there are two circumstances in which access may be restricted: if disclosure poses a risk of harm to the individual, or if it poses a risk of harm to others. Regional or national legislation governs these situations and outlines an individual’s right to appeal any denial to the appropriate Privacy Commissioner or regulatory authority.

The right to amend PHI allows individuals to challenge the accuracy or completeness of their information and request that an amendment be attached to the relevant document, clearly identifying the area of concern. The amendment must be written, signed, and dated by the

individual, specifying what they believe to be inaccurate or incomplete. Because a health record, whether paper or electronic, is a legal document, it cannot be altered or destroyed; however, an addendum may be permanently appended to the original record.

Any party that received the original information must also receive a copy of the addendum to ensure all holders of the record are aware of the correction. To maintain accountability, organizations should use a tracking log or disclosure register to document who accessed information, for what purpose, and when it was released. This ensures that any necessary amendments are appropriately communicated to all recipients.

If an organization becomes aware of a privacy breach involving unauthorized access to PHI, it is best practice, and, in some jurisdictions, a legal requirement to notify the affected individual immediately. The organization's privacy policy should clearly outline the procedures for breach notification, including timelines, responsible personnel, and reporting protocols.

x) 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?

Individuals must have the ability to question or challenge an organization's compliance with established privacy principles. Each healthcare organization that maintains Personal Health Information (PHI) is required to develop and implement a compliance policy and supporting procedures that outline how individuals or their representatives can raise privacy-related concerns or complaints.

Any such challenge should be directed to the designated Privacy Officer or equivalent authority within the organization. The Privacy Officer is responsible for investigating and responding to complaints, ensuring that appropriate corrective actions are taken when necessary, and maintaining documentation of all inquiries and resolutions.

Best practice is to make the complaint process transparent and easily accessible. Organizations should clearly display this information such as

on their website or in public areas so that individuals are aware of their right to challenge compliance and understand how to initiate the process.

VI. Security of Patient Information

A. Security Policies

Every healthcare organization must have processes and safeguards in place to protect the security of Personal Health Information (PHI). The methods used will vary depending on the size, scope, and complexity of the organization. At a minimum, each organization should maintain a comprehensive Security Policy that outlines its commitment to maintaining appropriate security standards and provides an overview of the strategies and controls implemented to achieve this.

Security breaches can occur in many forms, including leaving file room doors unlocked, sending patient information to the wrong fax number, leaving confidential documents unattended, or sharing passwords. Each of these actions increases the risk of unauthorized access or disclosure of PHI.

A clearly defined Security Policy serves as an essential guide for all staff,

establishing expectations for protecting patient information and helping departments create consistent procedures tailored to their functions. Health Information Management (HIM) professionals have both ethical and regulatory obligations to protect patient data and typically work closely with Information Technology (IT) departments to ensure systems and software that store, or process PHI are secure and compliant.

<u>Points to Consider Including Within a Security Policy</u>

- Security Goals and Principles: Outline the organization's guiding goals, such as maintaining the confidentiality, integrity, and availability of information.
- Roles and Responsibilities: Define the basic security and accountability expectations for all personnel, including staff, physicians, and volunteers.
- Privacy and Security Training: Require privacy and security education for all personnel at the time of hire and at least annually thereafter.

- Policy Review and Maintenance: Designate an individual responsible for regularly reviewing and updating the policy to ensure it remains current with evolving technologies and regulations.
- Access Controls: Describe how access to PHI is granted, managed, and protected, including user roles, password requirements, and access levels within electronic systems.
- Physical Safeguards: Identify the physical measures in place to control access to areas where PHI is stored and processed, such as locked file rooms and secure workstations.
- Vendor and Contractor Access: Establish procedures for managing and monitoring external vendors or contractors who may require access to PHI, ensuring they comply with organizational standards.
- Confidentiality Agreements: Require all personnel, contractors, and volunteers to sign a confidentiality agreement upon hire or engagement.
- Designation of a Privacy/Security Officer: Appoint a qualified individual responsible for overseeing privacy and security compliance across the organization.

B. Security and People

The effectiveness of any security program depends not only on technology but also on the people who use it. Even the most advanced systems can be compromised if staff members are not committed to protecting confidential patient information.

i) **Inform**, educate, and motivate personnel.

- Provide clear guidance and continuous education to ensure personnel understand their responsibilities. Training should emphasize the organization's security policies, physical security procedures, proper fax and email use, password protection, and how to report potential breaches or near misses.
- Perform appropriate screening for personnel who handle PHI, work within information systems, or hold positions with special security responsibilities.

- Require all personnel to sign and acknowledge the organization's confidentiality agreement, affirming their obligation to protect PHI.
- Implement privacy and security training at the time of hire and annually thereafter as part of the organization's continuing education program, alongside other key topics such as fire safety.

ii) **Impose** controls to establish clear rules that prevent unauthorized access to PHI.

- Access controls can be accomplished by following the steps detailed in the section above and by creating an organizational policy to limit access to PHI based on job roles and duties. For example, a billing clerk should not have access to a patient's operative report, while a treating physician should have full access to records relevant to patient care.
- Require vendors, contractors, and other third parties to sign confidentiality agreements such as a Business Associate Agreement (BAA) before being granted access to PHI or organizational systems.

C. Physical Security

All personnel must understand and uphold their responsibilities related to physical security, as these measures are essential to protecting Personal Health Information (PHI). Key physical guards must include:

- Keep doors to file rooms, record storage areas, and other secure locations always locked. Do not permit unauthorized individuals to enter areas where confidential information is stored.
- Never share passwords.
- Staff must log out or lock their workstation whenever it is unattended to prevent unauthorized access.

- Ensure that sensitive information is stored securely and handled appropriately, especially when transported outside the immediate work area.
- All staff should wear organizational identification badges, preferably with a photograph, indicating they are authorized to access secure areas.
- Paper-based PHI must be disposed of through approved methods, such as shredding or locked destruction bins.
- Collaborate with the Information Systems Department to implement technical safeguards, such as:
- Password-protected access to all computers and systems.
- Automatic screen savers with timeout functions to prevent unauthorized viewing.
- Proper monitor placement to avoid “shoulder surfing” by unauthorized individuals.
- Policies prohibiting the external emailing of PHI unless secure methods are used.

VII. Privacy Breaches

A privacy breach in a healthcare setting can have serious consequences. Many jurisdictions impose significant financial and disciplinary penalties—particularly for intentional or malicious breaches of Personal Health Information (PHI). Breaches can take many forms, including sending a fax to the wrong number, theft or loss of a device containing PHI, unauthorized access or “snooping” into patient records, or the inappropriate disclosure or sale of patient information.

Every organization should maintain a comprehensive “Breach Management Policy” that outlines the steps required to investigate and document a breach. This policy should guide staff through the reporting process, identify responsible parties, and specify how findings will be communicated. Moreover, the Human Resources Department should maintain a “Discipline Policy” that defines the consequences of privacy breaches, considering both the severity and the intent of the incident. Serious, intentional, or malicious breaches of patient information should result in termination of employment in accordance with best practices and regulatory expectations.

VIII. Emerging Threats and Cybersecurity

Healthcare systems and the information they manage are increasingly targeted by malicious actors, hackers, and cybercriminals. Maintaining a strong cybersecurity posture requires ongoing vigilance to protect the confidentiality, integrity, and availability of Personal Health Information (PHI).

The exchange of information across healthcare, insurance, and government agencies can introduce vulnerabilities if not properly managed. Inadequate safeguards may place patients at risk and potentially lead to significant harm.

The frequency and sophistication of cyberattacks on healthcare organizations have risen dramatically worldwide. Breaches may result from malicious insiders, unauthorized access, hacking incidents, theft, or improper disposal of records or equipment containing PHI.

Cybersecurity attacks on healthcare have increased dramatically around the world resulting in a greater number of data breaches. This is either from malicious insiders, theft, unauthorized access, hacking and improper disposal of information.

The growing use of electronically controlled medical devices, wearable technologies, and digitally managed care processes adds additional layers of complexity and increases the potential for cyber risk.

Healthcare organizations must be proactive in strengthening their cybersecurity frameworks. This includes conducting regular security audits, vulnerability assessments, and penetration testing to identify and address weaknesses. Implementing these measures is essential to maintaining patient trust and safeguarding critical data and assets.

IX. Summary

This unit explored the critical role of Health Information Management (HIM) professionals in safeguarding sensitive patient information. As custodians of Personal Health Information (PHI), HIM professionals must be knowledgeable about the full range of privacy and security considerations they will encounter throughout their careers. In many organizations, they also hold responsibility for overseeing privacy and security programs, policies, and compliance activities.

HIM professionals are recognized for their expertise in regulatory requirements, ethical standards, and best practices related to the protection of PHI. Their work is grounded in a strong ethical Code of Conduct that requires them to uphold privacy and confidentiality at all times.

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 always uphold and maintain PHI.

This unit provided a high-level overview of the principles, obligations, and strategies that support the secure management, protection, and disclosure of PHI across healthcare settings.

X. Review Questions

1. If you are an HIM Coder and notice that your neighbor has been brought into the Emergency Department, is it appropriate for you to access their patient chart?
2. Is it permissible to sell patient names to a third party for marketing purposes (e.g., baby formula advertisements for new parents)?
3. A famous athlete is admitted to your hospital. If a local newspaper calls requesting information about their condition, is it acceptable for you to provide details?
4. Is it appropriate to discuss patient information in public areas such as hallways, elevators, or waiting rooms?
5. If a co-worker asks for your login credentials so they can access a patient's electronic health record, should you share your password?
6. Is it acceptable to leave the file room door unlocked?
7. How many universal privacy principles are there?
8. A patient's husband arrives at the Health Information Management Department requesting copies of his wife's medical records and states he will sign on her behalf. Is this permissible?

XI. 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)
6. Alanazi AT. Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. Cureus. 2023 Oct 14;15(10):e47026. doi: 10.7759/cureus.47026. PMID: 37965389; PMCID: PMC10642560.