Course: Health Records Management

Lecture: 9 Security and Confidentiality of Health Information

Lecturer: Dr. Johnson Masinde

9.1 Introduction

Security and confidentiality of health information are fundamental principles in **health records management** that safeguard patients' personal, medical, and demographic data from unauthorized access, misuse, alteration, or disclosure. In the digital era, where healthcare systems increasingly rely on **Electronic Health Records (EHRs)** and other information technologies, protecting health information has become a critical ethical, legal, and operational concern.

Health information security refers to the policies, technologies, and procedures implemented to ensure that health data is **protected from threats**, including loss, damage, or unauthorized access. **Confidentiality**, on the other hand, involves the ethical and legal duty of healthcare providers to protect patient information from unauthorized disclosure. Together, these principles preserve **patient trust**, support **effective healthcare delivery**, and ensure **compliance** with national and international standards such as the **Kenya Data Protection Act (2019)**, **HIPAA (Health Insurance Portability and Accountability Act)**, and **ISO 27799** on health informatics security.

Ensuring data security and confidentiality helps to maintain **integrity**, **availability**, and **privacy** of information, which are crucial for high-quality healthcare, ethical conduct, and institutional accountability.

This topic is divided into four key **s**ubtopics, namely:

1. Concept and Principles of Health Information Security and Confidentiality
2. Threats and Risks to Health Information Security
3. Measures and Technologies for Protecting Health Information
4. Legal and Ethical Frameworks Governing Health Information Security and Confidentiality

Expected Learning Outcomes

By the end of this topic, students should be able to:

1. **Explain the key concepts and principles** of health information security and confidentiality.
2. **Identify and analyze the major threats and risks** affecting the security of health information in healthcare organizations.
3. **Discuss various measures and technologies** used to protect the security and confidentiality of health records.
4. **Evaluate legal and ethical frameworks** that guide the protection of health information at national and global levels.
5. **Recommend best practices** for strengthening security and confidentiality in both manual and electronic health record systems

The key concepts in this topic include:

1. Health Information Security: This involves implementing appropriate **administrative, physical, and technical safeguards** to protect health information against unauthorized access, disclosure, or loss. It ensures **data integrity**, **availability**, and **confidentiality** throughout the information lifecycle from creation to disposal.

2. Confidentiality of Health Information: Confidentiality refers to the **ethical and legal obligation** of healthcare providers and institutions to protect patient information from being shared or accessed without proper authorization. It fosters **trust between patients and healthcare providers**, encouraging full disclosure during medical consultations, which is vital for accurate diagnosis and treatment.

3. Privacy vs. Confidentiality: While **privacy** relates to the right of individuals to control access to their personal information, **confidentiality** refers to the duty of healthcare workers to keep patient information secret. Both are essential for maintaining professional ethics and public confidence in healthcare services.

4. Importance of Security and Confidentiality: Maintaining data security and confidentiality ensures **compliance with legal regulations**, **protection of patient rights**, **prevention of data breaches**, and **enhancement of data quality and trust** in healthcare systems. Breaches can lead to identity theft, legal liabilities, reputational damage, and loss of public trust.

Therefore, **security and confidentiality of health information** are cornerstones of modern health information management. They not only protect patient rights but also enhance the **efficiency, accountability, and ethical standing** of healthcare institutions. Through proper policies, secure technologies, and adherence to ethical standards, health professionals can ensure that patient information remains **safe, confidential, and reliable** in both digital and physical formats.

9.2 Concept and Principles of Health Information Security and Confidentiality

Health information security and confidentiality form the foundation of ethical and professional health records management. They ensure that patient data is handled responsibly, safely, and in compliance with both **legal and ethical standards**. In an era where health systems rely heavily on **digital technologies and electronic health records (EHRs)**, protecting health information from misuse, unauthorized access, and cyber threats has become increasingly crucial. The concept and principles of security and confidentiality aim to maintain **patient trust**, support **clinical accuracy**, and uphold the **integrity** of healthcare systems.

Concept of Health Information Security

Health information security refers to the set of measures, policies, and technologies designed to protect health data from unauthorized access, alteration, destruction, or disclosure. It ensures that information remains **confidential, available, and accurate** throughout its lifecycle. The security of health information is guided by the **CIA triad model**, which stands for **Confidentiality, Integrity, and Availability**.

Confidentiality ensures that only authorized persons can access patient data. **Integrity** guarantees that information remains accurate, consistent, and unaltered during storage, processing, and transmission. **Availability** ensures that data is accessible to authorized users when needed for

clinical decision-making and patient care. Together, these principles ensure that patient information is used ethically, stored securely, and shared appropriately.

Security involves three major components: **administrative, physical, and technical safeguards.**

- **Administrative safeguards** include policies, procedures, and staff training aimed at ensuring compliance with data protection regulations.
- **Physical safeguards** involve securing physical locations such as file rooms, storage areas, and computer facilities to prevent unauthorized access.
- **Technical safeguards** include the use of passwords, encryption, firewalls, and access control systems to secure electronic data.

Concept of Confidentiality in Health Information

Confidentiality refers to the obligation of healthcare providers and institutions to protect patient information from unauthorized access, use, or disclosure. It is based on the ethical principle of **respect for patient privacy and autonomy**, ensuring that personal information shared during medical care is used solely for legitimate purposes.

Confidentiality builds **trust between patients and healthcare providers**, which is essential for effective diagnosis and treatment. When patients trust that their data is secure, they are more likely to share complete and accurate information, which improves the quality of healthcare. Violation of confidentiality can lead to loss of trust, legal consequences, and reputational damage to the institution.

To maintain confidentiality, access to health records should be **restricted to authorized personnel** only. Information should be shared strictly on a need-to-know basis and in accordance with institutional policies and legal frameworks. In the case of electronic records, additional protections such as **encryption, secure logins, and audit trails** are essential to prevent unauthorized access.

Principles of Health Information Security and Confidentiality

1. **Confidentiality Principle** – Health information should be accessible only to authorized individuals. This principle protects patients from the misuse of their personal health data and ensures compliance with data protection laws.
2. **Integrity Principle** – Health data must remain complete, accurate, and unaltered. This principle ensures that records are reliable for clinical, administrative, and legal purposes. Unauthorized alteration or tampering compromises data quality and may lead to medical errors.
3. **Availability Principle** – Authorized healthcare personnel should have timely and reliable access to patient data whenever needed. This supports effective service delivery, continuity of care, and informed decision-making.
4. **Accountability Principle** – Every individual handling health records must be responsible for maintaining data security and confidentiality. Institutions should implement policies that define user roles, assign responsibilities, and track access to health data.
5. **Transparency and Consent Principle** – Patients should be informed about how their data is collected, stored, used, and shared. Their consent should be obtained before sharing health information, except in legally permissible situations such as public health surveillance or court orders.
6. **Compliance with Legal and Ethical Standards** – Health institutions must adhere to national laws such as the **Kenya Data Protection Act (2019)**, the **Health Act (2017)**, and international standards like **HIPAA** and **ISO 27799**. These frameworks provide guidelines on data handling, security measures, and penalties for breaches.
7. **Minimum Necessary Use Principle** – Only the minimum amount of health information necessary for a specific purpose should be disclosed. This principle prevents unnecessary exposure of patient data and minimizes risks of breaches.

Importance of Health Information Security and Confidentiality

Maintaining the security and confidentiality of health information is essential for several reasons. It **protects patient privacy and autonomy**, which are fundamental rights in healthcare. It also

enhances trust between patients and healthcare providers, encouraging honest communication and accurate disclosure of health information.

Furthermore, strong security measures **prevent data breaches and cyberattacks**, safeguarding institutions from legal penalties and financial losses. Data protection also **improves the quality and reliability** of health records, ensuring that medical decisions are based on accurate and complete information.

Challenges in Maintaining Security and Confidentiality

Despite the importance of data security, healthcare organizations face challenges such as **inadequate infrastructure, lack of staff training, weak enforcement of policies, and increasing cyber threats.** Paper-based records may be lost or damaged, while electronic systems are vulnerable to hacking and unauthorized access. Addressing these challenges requires a combination of **technical solutions**, **policy enforcement**, and **capacity building** among health information professionals.

In summary, the **concept and principles of health information security and confidentiality** emphasize the protection of patient data from unauthorized access and misuse. They uphold ethical, legal, and professional standards in health records management, ensuring that information remains reliable, accurate, and accessible only to authorized personnel. By applying the principles of confidentiality, integrity, availability, accountability, and compliance, healthcare institutions can maintain public trust, support quality healthcare, and ensure compliance with national and international regulations.

9.3 Threats and Risks to Health Information Security

Health information security is constantly threatened by a variety of risks that can compromise the **confidentiality, integrity, and availability** of patient data. In healthcare environments, both **internal and external threats** can lead to unauthorized access, loss, or manipulation of sensitive health records. These risks have grown with the increased use of **Electronic Health Records (EHRs)**, digital storage systems, and networked databases. Understanding the types of threats and

risks to health information security is crucial for developing effective **preventive and mitigation strategies** to protect patient information and ensure compliance with **legal and ethical standards**.

Types of Threats and Risks to Health Information Security

1. Human Threats

Human factors pose the most significant threat to the security of health information. These may occur due to **negligence, lack of training, or malicious intent.**

- **Unauthorized access:** Employees or outsiders accessing patient records without proper authorization.
- **Human error:** Mistakes such as accidental deletion, incorrect data entry, or mishandling of records.
- **Insider threats:** Staff members intentionally misusing or leaking patient information for personal or financial gain.
- **Social engineering:** Attackers manipulate staff through deception (e.g., phishing) to gain access to confidential data.

  These threats highlight the importance of **training**, **access control**, and **awareness programs** to foster a culture of information security.

2. Technical Threats

Technical threats arise from vulnerabilities in **computer systems, networks, and software applications** used to store and transmit health data.

- **Malware and viruses:** Malicious software can corrupt files, steal data, or disrupt system operations.
- **Ransomware attacks:** Cybercriminals encrypt patient data and demand ransom payments for restoration.
- **System hacking:** External attackers exploit security loopholes to gain unauthorized access to EHR systems.
- **Data breaches:** Occur when sensitive patient data is exposed due to poor security configurations or outdated software.

- **Unsecured mobile devices and cloud systems:** Health workers accessing data via personal or unprotected devices pose significant security risks. Technical threats can be minimized through **encryption, firewalls, intrusion detection systems, and regular software updates**.

3. Physical Threats

Physical threats involve damage or unauthorized access to health information due to **environmental or physical factors.**

- **Theft or loss of equipment:** Laptops, flash drives, and other portable storage devices containing health data may be lost or stolen.
- **Fire, floods, or natural disasters:** Physical damage to storage facilities or computer servers can result in data loss.
- **Unauthorized physical access:** Uncontrolled access to file rooms or server areas may lead to tampering or theft of records.
  Effective **facility management**, **secure storage**, and **disaster recovery planning** are essential to mitigate these risks.

4. Organizational and Policy Threats

Weak institutional policies or poor governance structures can create vulnerabilities that compromise health data security.

- **Absence of security policies:** Lack of comprehensive data protection policies leads to inconsistent handling of sensitive information.
- **Weak enforcement mechanisms:** Policies may exist but remain unimplemented or ignored due to lack of accountability.
- **Inadequate training and awareness:** Staff may not fully understand their roles and responsibilities in protecting patient information.
- **Poor record management systems:** Disorganized filing systems and lack of audits increase the likelihood of data mishandling.
  To address these issues, organizations should adopt **standard operating procedures (SOPs)**, conduct **regular audits**, and implement **continuous staff training programs**.

5. Environmental and Natural Risks

Health records, whether physical or electronic, are also vulnerable to **environmental hazards** and **natural disasters.**

- **Fire outbreaks, floods, or earthquakes:** Can destroy physical records or damage computer systems and backup servers.
- **Power outages:** May lead to loss of unsaved data or disrupt access to critical information systems.
- **Poor storage conditions:** Excessive humidity, pests, or dust can damage paper records, while heat can affect electronic devices.

  Organizations must develop **business continuity and disaster recovery plans** to ensure health data protection in case of emergencies

6. Legal and Ethical Risks

Violations of laws and ethical standards concerning data protection can pose serious threats to healthcare institutions.

- **Non-compliance with data protection regulations** such as the **Kenya Data Protection Act (2019)** or **HIPAA** can lead to legal sanctions, financial penalties, and reputational damage.
- **Improper disclosure of patient information** without consent breaches ethical codes and patient trust.
- **Failure to implement adequate safeguards** can expose institutions to lawsuits and loss of accreditation.

  Healthcare institutions must implement **legal compliance frameworks**, conduct **regular risk assessments**, and ensure **adherence to ethical codes of practice** in handling patient information.

Consequences of Threats to Health Information Security

Failure to address security risks can have severe consequences, including:

- **Loss of patient trust** and reluctance to disclose accurate health information.

- **Legal liabilities** resulting from data breaches or non-compliance with regulations.
- **Financial losses** due to fines, lawsuits, or ransomware payments.
- **Disruption of healthcare services** if systems become inaccessible or compromised.
- **Reputational damage** that undermines public confidence in the healthcare institution.

Mitigation and Prevention Strategies

To reduce risks, healthcare organizations should adopt a **multi-layered security approach** combining administrative, physical, and technical safeguards.

- Develop and enforce **data security policies** aligned with national and international standards.
- Implement **role-based access control** and regular password changes to limit unauthorized access.
- Conduct **periodic risk assessments and audits** to identify vulnerabilities.
- Use **encryption, antivirus software, and firewalls** to protect digital systems.
- Provide **continuous staff training** on data protection, confidentiality, and ethical handling of patient information.
- Maintain **backup systems and disaster recovery plans** to ensure data continuity.

The **threats and risks to health information security** are diverse, ranging from human errors and cyberattacks to natural disasters and weak institutional policies. Protecting patient data requires a proactive and comprehensive approach that integrates **technological, administrative, physical, and legal safeguards.** By addressing these threats, healthcare institutions can preserve the confidentiality, integrity, and availability of health information thereby ensuring ethical compliance, protecting patient rights, and maintaining public trust in the healthcare system.

9.4 Measures and Technologies for Protecting Health Information

The protection of **health information** is a critical component of modern healthcare management. As health institutions increasingly rely on **electronic health records (EHRs)** and digital systems, the need to safeguard patient data from unauthorized access, alteration, and loss has become paramount. Effective protection of health information involves the integration of **administrative,**

physical, and technical measures supported by robust **technological solutions**. These strategies ensure that patient data remains **confidential, accurate, and accessible** only to authorized individuals.

The implementation of these protective measures not only ensures **compliance with legal and ethical standards** but also enhances **patient trust, institutional accountability, and healthcare service delivery.**

1. Administrative Measures

Administrative measures refer to the policies, procedures, and management practices designed to protect health information within an organization. These form the foundation for data governance and employee accountability.

- **Development of Policies and Procedures:** Clear policies on data access, use, sharing, and storage help define staff responsibilities and ensure uniform practices. Policies should align with legal frameworks such as the **Kenya Data Protection Act (2019)** and international standards like **HIPAA** and **ISO 27799**.
- **Access Control Policies:** These define who can view, modify, or share health information. Access should be based on the principle of **least privilege**, allowing users to access only the data necessary for their role.
- **Staff Training and Awareness:** Regular training sessions educate healthcare staff about data protection, cybersecurity awareness, and ethical responsibilities in handling patient information.
- **Confidentiality Agreements:** Employees should sign confidentiality or non-disclosure agreements as part of their employment terms to emphasize accountability in data protection.
- **Auditing and Monitoring:** Routine audits help identify potential security weaknesses, detect unauthorized access, and ensure adherence to data protection standards.
- **Incident Response Planning:** Every health organization should have a defined procedure for detecting, reporting, and mitigating data breaches or security incidents.

2. Physical Measures

Physical measures involve the protection of health information from environmental hazards, theft, or unauthorized physical access. These measures are critical in both paper-based and electronic health record systems.

- **Controlled Access:** Restrict entry to health record rooms, server areas, and offices using access badges, biometric systems, or security personnel.
- **Secure Storage:** Paper records should be kept in lockable cabinets or archives, while electronic devices should be stored in secure environments protected from unauthorized users.
- **Environmental Controls:** Use fireproof cabinets, smoke detectors, air conditioning, and humidity controls to protect physical records and IT infrastructure from environmental damage.
- **Surveillance and Security Systems:** Install surveillance cameras and alarms in record storage areas to monitor and deter unauthorized entry.
- **Backup Power and Disaster Recovery Facilities:** Use uninterruptible power supplies (UPS) and generators to prevent data loss during power outages. Offsite backup facilities ensure recovery in case of natural disasters such as fires or floods.

Physical measures are essential for maintaining the **availability and integrity** of health information in all formats.

3. Technical Measures

Technical measures encompass digital and technological safeguards that secure electronic health information systems from unauthorized access, corruption, or cyberattacks.

- **Data Encryption:** Encryption converts health information into unreadable code, ensuring that even if data is intercepted, it remains inaccessible to unauthorized individuals.
- **Firewalls and Intrusion Detection Systems:** Firewalls filter network traffic, blocking unauthorized access, while intrusion detection systems (IDS) monitor and alert administrators of suspicious activities.

- **User Authentication and Authorization:** Employ strong password policies, multi-factor authentication (MFA), and biometric verification to confirm user identities before granting access to data.
- **Role-Based Access Control (RBAC):** Limits system access to specific users based on their job responsibilities, minimizing the risk of internal data misuse.
- **Data Backup and Recovery Systems:** Regular data backups stored both onsite and offsite ensure that information can be restored in case of accidental loss or cyber incidents such as ransomware attacks.
- **Antivirus and Anti-Malware Software:** These protect systems against viruses, malware, and other malicious programs that can corrupt or steal data.
- **Secure Communication Channels:** Use encrypted email systems, secure cloud platforms, and Virtual Private Networks (VPNs) to protect information transmitted across networks.

Technical measures are vital in ensuring **data integrity, confidentiality, and system reliability** in digital healthcare environments.

4. Emerging Technologies for Health Information Protection

Rapid technological advancements have introduced innovative tools to enhance health data protection.

- **Blockchain Technology:** Provides a decentralized, tamper-proof ledger for recording health transactions, enhancing data integrity and traceability.
- **Artificial Intelligence (AI) and Machine Learning (ML):** Used to detect anomalies, identify security breaches, and predict potential vulnerabilities in health information systems.
- **Cloud Security Solutions:** Secure cloud platforms allow institutions to store and manage data remotely, with advanced encryption and access control features.
- **Data Masking and Tokenization:** Protects sensitive patient data by replacing identifiable information with pseudonyms or random tokens during analysis or transfer.
- **Zero Trust Security Models:** Require continuous verification of every user and device attempting to access health systems, minimizing risks of internal and external breaches.

These emerging technologies strengthen traditional security methods and ensure adaptive protection against evolving cyber threats.

5. Legal and Regulatory Compliance Measures

Ensuring protection of health information also involves adherence to national and international data protection frameworks.

- In **Kenya**, institutions must comply with the **Kenya Data Protection Act (2019)**, which mandates data minimization, secure storage, and accountability in personal data handling.
- Globally, standards such as **HIPAA (1996)** in the United States, **GDPR (2018)** in the European Union, and **ISO 27799** guide healthcare organizations in implementing security and confidentiality controls.
- Compliance audits, documentation, and certifications help demonstrate an organization's commitment to ethical and legal data management.

Compliance ensures that institutions are **accountable, transparent, and legally protected** in their health information management practices.

6. Organizational Best Practices for Data Protection

Healthcare institutions can strengthen data protection by implementing the following best practices:

- Establishing a **data governance committee** to oversee security policies and compliance.
- Conducting **regular risk assessments** to identify and mitigate emerging threats.
- Promoting a **security culture** through staff sensitization and continuous training.
- Maintaining an updated **inventory of all data assets** to track where sensitive health information is stored.
- Performing **periodic penetration testing** to identify weaknesses in information systems.

These practices ensure a proactive approach to safeguarding health information and maintaining compliance with global standards.

Effective protection of health information requires a **multifaceted approach** combining administrative, physical, and technical measures reinforced by emerging technologies. By integrating these safeguards, healthcare organizations can maintain **confidentiality, integrity, and availability** of patient data while meeting **legal and ethical obligations**. Strong security measures not only prevent data breaches but also **enhance patient trust**, **improve healthcare outcomes**, and **promote organizational accountability** in the management of sensitive health information.

9.5 Legal and Ethical Frameworks Governing Health Information Security and Confidentiality

Legal and ethical frameworks play a critical role in ensuring that the collection, storage, use, and sharing of health information are conducted responsibly and in accordance with established laws, professional standards, and societal values. These frameworks establish **obligations for healthcare professionals, institutions, and data handlers** to protect patients' privacy, uphold confidentiality, and maintain the security of health information throughout its lifecycle.

Health information is sensitive and personal; therefore, it must be managed in compliance with **national regulations, international conventions, and ethical principles** that govern how such data can be used, shared, and protected. These frameworks not only define **patients' rights** but also outline **institutional responsibilities**, penalties for non-compliance, and procedures for ensuring accountability and transparency in information handling.

Legal Frameworks Governing Health Information Security and Confidentiality

Legal frameworks consist of laws, policies, and regulations that establish the **rules and standards** for protecting health data. These frameworks ensure that healthcare organizations implement measures to prevent unauthorized access, disclosure, and misuse of information.

1. Kenya Data Protection Act (2019):

This Act provides the legal foundation for data privacy and protection in Kenya. It governs the **collection, processing, storage, and sharing** of personal data, including health information. It emphasizes principles such as **lawfulness, fairness, transparency, purpose limitation, data minimization, and accountability**. The Act also establishes the **Office of the Data Protection Commissioner (ODPC)** to enforce compliance and protect citizens' data rights.

2. Health Information Systems Policy (Kenya, 2016):

This policy supports the management and security of health information within Kenya's health system. It promotes the use of **standardized systems and interoperability**, while ensuring data protection, ethical use, and confidentiality of patient records.

3. The Health Act (2017):

The Health Act emphasizes the **confidential handling of patient information** by all health workers and facilities. It outlines the rights of patients to privacy and stipulates penalties for unauthorized disclosure or misuse of health information.

4. International Legal Frameworks:

Globally, countries adhere to legal standards such as:

- **HIPAA (Health Insurance Portability and Accountability Act, USA):** Protects patient health information by setting national standards for electronic healthcare transactions and the protection of personal data.
- **GDPR (General Data Protection Regulation, EU):** Sets strict rules on how organizations collect, process, and store personal data, including health information. It gives individuals greater control over their personal information.
- **ISO 27799:2016 (Health Informatics — Information Security Management in Health):** Provides guidelines for managing information security in health using **ISO/IEC 27002** as a foundation.

These international laws influence national policies and establish best practices for health data protection.

Ethical Frameworks Governing Health Information Security and Confidentiality

Ethical frameworks are based on moral principles that guide the behavior of healthcare professionals in managing patient information. They emphasize respect for human dignity, trust, and responsibility.

1. Principle of Confidentiality:

Healthcare professionals have an **ethical obligation** to maintain confidentiality by not disclosing patient information without consent. This principle is rooted in the **Hippocratic Oath** and reinforced by professional codes of conduct such as those of the **World Medical Association (WMA)**.

2. Principle of Autonomy:

Patients have the **right to control** their personal health information. They must be informed about how their data is collected, stored, used, and shared, and have the ability to grant or withdraw consent.

3. Principle of Beneficence and Non-Maleficence:

Health professionals must act in the **best interest of the patient (beneficence)** while avoiding actions that could cause harm (**non-maleficence**), including breaches of confidentiality or data misuse.

4. Principle of Justice:

This principle ensures **fair and equitable treatment** in data handling. Health information should not be used to discriminate or stigmatize patients based on gender, disease, or socioeconomic status.

5. Professional Codes of Ethics:

Professional organizations such as the **Health Records and Information Managers Association (HRIMA)** and the **International Federation of Health Information Management Associations (IFHIMA)** require members to adhere to ethical standards of privacy, confidentiality, and professional integrity in managing health information.

Integration of Legal and Ethical Frameworks

For effective management of health information, **legal and ethical frameworks must complement each other**. Laws provide enforceable standards, while ethical principles guide moral behavior and professional judgment. Compliance with both ensures that health data is

managed responsibly, patients' rights are protected, and healthcare institutions maintain public trust.

Healthcare organizations must therefore:

- Develop and implement **privacy and confidentiality policies** aligned with both legal and ethical requirements.
- Conduct **training and awareness programs** for staff on ethical data handling.
- Establish **data protection officers or committees** to ensure compliance and accountability.
- Regularly **audit and monitor** data access and usage to detect and prevent breaches.

Legal and ethical frameworks are indispensable in safeguarding the **security and confidentiality of health information**. They form the foundation for trust, accountability, and professionalism in healthcare. By adhering to both national and international laws, as well as ethical standards, healthcare institutions can ensure that health information remains **secure, confidential, and used solely for the benefit of patient care and public health advancement**.

Self-Assessment Questions

1. Explain the key principles of health information security and confidentiality and discuss their relevance in modern healthcare environments.
2. Identify and analyze major threats and risks that compromise the security and confidentiality of health information in both paper-based and electronic systems.
3. Discuss the measures and technologies that healthcare institutions can implement to enhance the protection of sensitive health data.
4. Examine the legal and ethical frameworks that govern health information security and confidentiality, highlighting their significance in ensuring compliance and professional responsibility.
5. Evaluate the challenges and best practices in maintaining security and confidentiality of health information within the context of digital transformation and data sharing in healthcare.

References

1. ISO. (2016). *ISO 27799: Health Informatics — Information Security Management in Health Using ISO/IEC 27002.* International Organization for Standardization.
2. Kenya Data Protection Act. (2019). *Laws of Kenya: An Act of Parliament to Provide for the Regulation of the Processing of Personal Data.* Government Printer.
3. U.S. Department of Health and Human Services. (1996). *Health Insurance Portability and Accountability Act (HIPAA).* Washington, D.C.
4. World Health Organization (WHO). (2017). *Guidelines on Ethical Issues in Public Health Surveillance.* Geneva: WHO Press.
5. International Federation of Health Information Management Associations (IFHIMA). (2020). *Ethical Standards for Health Information Management Professionals.* IFHIMA Publications.