

# **Course: Health Records Management**

## **Lecture: 5 Answers to Self-Assessment Questions**

**Lecturer: Dr. Johnson Masinde**

- 1) **Discuss the importance of data privacy and confidentiality in health records management, and explain the consequences of breaches.**

Data privacy and confidentiality are fundamental in health record management because health records contain highly sensitive information such as patient history, diagnoses, treatments, and personal identifiers. Protecting confidentiality preserves patient trust, ensures compliance with legal frameworks, and upholds ethical standards in healthcare. Breaches can lead to severe consequences including identity theft, stigmatization, financial fraud, loss of patient trust, and reputational damage to healthcare providers. In addition, legal penalties such as fines and sanctions may be imposed under regulations like HIPAA or GDPR.

- 2) **Explain how legal frameworks such as HIPAA, GDPR, or local data protection laws influence the management of health records.**

Legal frameworks provide a structured basis for how health information should be collected, stored, accessed, and shared. For example, HIPAA in the U.S. establishes strict requirements for safeguarding patient information and limits unauthorized disclosures. The GDPR in Europe provides patients with rights such as data access, correction, and the “right to be forgotten.” These laws influence policies, procedures, and technical safeguards in healthcare institutions. Locally, data protection acts often mandate security measures, retention policies, and penalties for noncompliance. These frameworks ensure accountability and uniformity in health records management.

- 3) **What are the key ethical principles that guide health record management, and how do they apply in daily healthcare practice?**

The main ethical principles include:

- **Confidentiality:** Ensuring that patient information is not disclosed without proper authorization.

- **Autonomy:** Respecting patients' rights to make informed decisions about the use of their health data.
- **Beneficence:** Using health data in ways that promote the well-being of patients and society, such as in treatment or research.
- **Non-maleficence:** Avoiding harm by preventing misuse or mishandling of health data. In daily practice, these principles apply through careful handling of medical records, obtaining informed consent, ensuring secure data storage, and limiting access to only authorized personnel.

4) **Identify at least three challenges healthcare institutions face in maintaining both legal compliance and ethical standards in health record management.**

- **Data Breaches and Cybersecurity Threats:** The increasing use of electronic health records exposes institutions to risks of hacking, unauthorized access, or accidental disclosures.
- **Complex and Evolving Legal Requirements:** Healthcare providers must comply with multiple overlapping laws and regulations, which can be difficult to interpret and apply consistently.
- **Balancing Privacy with Public Health Needs:** Providers often face dilemmas when public health demands (e.g., during pandemics) require disclosure of patient data that conflicts with confidentiality. Other challenges include limited resources, lack of staff training, and ethical concerns surrounding emerging technologies like artificial intelligence in healthcare.

5) **Suggest best practices that can help healthcare organizations balance patient rights with the need for data sharing in research and public health.**

Best practices include:

- **De-identification and Anonymization:** Removing personal identifiers from datasets to protect individual privacy while enabling secondary use of data.
- **Robust Consent Processes:** Ensuring patients understand how their data may be used, including for research or public health, and providing them with the right to opt out.

- **Clear Data Sharing Agreements:** Establishing contracts that specify how shared data will be used, stored, and protected.
- **Transparency and Patient Engagement:** Communicating openly with patients about data use builds trust and acceptance.
- **Strong Data Governance Frameworks:** Implementing clear policies, monitoring, and oversight mechanisms ensures both legal compliance and ethical responsibility