EXAM OBJECTIVES

The following objectives are covered by the exam:

1. The Health Information System

General concepts

- Understanding the differences between data and information, and between computer systems and information systems.

- Identifying the characteristics and purposes of the Health Information System (HIS) and the New Health Information System (NHIS).

- Recognizing the territorial extension of the HIS: international, national, local, and medical or surgery.

- Understanding the characteristics, objectives, and benefits of a business information system for Hospital Resource Planning (HRP).

- Knowing that the HIS is a support tool for medical staff in decisions about the diagnosis and treatment of patients, based on timely, accurate, relevant, comprehensive, synthesized, and usable information.

- Appreciating the importance of validation of introduced data and recognizing the procedures.

- Recognizing the role of the HIS as a Decision Support System (DSS) and a powerful tool that does not replace the health worker in the decision process or responsibility.

- Recognizing that the HIS system the patient and the process of care in a central location facilitates the patients' access to their own data, provides for continuity of support, ensures access to resources, allows rigorous and documented application of precise guidelines, and sets the basis for the application of Evidence Based Medicine (EBM).

- Knowing the limits of an the HIS that can diminish and generalize the relationship between the healthcare worker and the patient through the introduction of technological instruments.

2. Management of personal patient data within the Health Information System

Management of confidential information

- Understanding which personal data is sensitive.

- Recognizing patients' rights: informative reports, contents, and consensus.

- Knowing who is entitled to give consent.

- Identifying the roles of key figures involved in the Privacy Code: Owner, Manager, Officer, and Interested.

- Understanding the purpose, method, and characteristics of the processing of personal data.

- Knowing the operations in the processing of personal data: collection, recording, organization, consulting, development, modification, selection, extraction, comparison, use, interconnection, blocking, communication, dissemination, erasure, and destruction of data.

- Recognizing the responsibility of the healthcare worker and the right to patient privacy.

Secure management of personal data

- Understanding the Programmatic Document on Security (PDS): what the PDS is useful for, when it is required to adopt it, who draws it up, and its periodic updating.

- Recognizing the minimum security measures aimed at reducing the risks of: destruction or loss of data, unauthorized access, treatment not allowed or not in accordance with the purposes of collection, data changes as a result of non-authorization, or non-conformity with the rules.

- Knowing the minimum security measures when processing sensitive data through IT tools.

- Recognizing the appropriate security measures aimed at reducing risks.

- Understanding information authentication: verification and validation of the identity of people accessing the treatment of personal data.

- Identifying the authentication credentials for access control of authorized people. Credentials are based on what the person knows (e.g., a password), has (e.g., a smart card), or is (e.g., a biometric characteristic, such as fingerprint, face, retina).

- Recognizing the assigned and associated credentials.

IC HEALTH

CERTIPORT®

- Describing the composition and usage guidelines of a password in order to reach a minimum level of security.

- Understanding the importance of the authorization system and authorization profile of the individual in charge of similar classes.

- Recognizing the measures of protection for electronic instruments and data concerning the risk of viruses, worms, Trojans, malware code, hackers and personnel with an unsuitable authorization profile.

- Understanding the importance of data rescue and disaster recovery to restore the normal operation of data processing.

Responsibilities and sanctions

- Understanding criminal responsibilities, sanctions, illegal processing of personal data, false statements to the guarantor, non-adoption of safety measures, and not following the requirements of the guarantor.

- Knowing civil responsibilities, administrative penalties, omitted or incomplete reports to officials, illegal transferring of data, omitted or incomplete notification, and failure to inform or submit documents to the guarantor.

3. Healthcare records

General concepts

- Understanding that a healthcare record is a collection of documents that record a heterogeneous complex of information on health, age, social status, and who is responsible for creating the diagnostic-therapeutic path for a patient, so that appropriate health interventions can be provided and scientific studies conducted, including statistics and medical conditions.

- Appreciating that a healthcare record is based on honor, questionable only when the data is shown to be false.

- Recognizing that the information on a healthcare record must be clear, concise, complete, legible, and understandable, with no deletions or omissions. It must be in chronological order without gaps, and corrections must be legible, dated, and signed.

- Knowing the advantages and disadvantages of paper healthcare records.

Computerized healthcare records

- Understanding the objectives of computerized healthcare records: to provide a needed piece of information; when, how, and where it is needed; to whom it is provided; and if he or she has authorization.

- Knowing the characteristics of computerized healthcare records, their advantages and disadvantages, and how they differ from paper records.

- Identifying the risk of intrusion, tampering, and destruction or loss of data, even if it is accidental, unauthorized, or not in accordance with the purposes of collecting the data, and information authentication and management of credentials for accessing data in a computerized folder.

- Indicating the types of data included in computerized folders and those who enter or use them: doctors, nurses, administrators, and management.

- Recognizing the importance of healthcare records for research, training, and documentation in health policy and management of resources.

Operative functions

- Recognizing the sections of a computerized healthcare record: age, acceptance, medical history, examination, clinical daily diary, action items, and dismissed items.

- Searching for the medical healthcare record of a patient and selecting a group of folders corresponding to specified search criteria.

- Identifying the author of data placed in a folder.

- Entering data into a folder.

- Making patient appointments for visits or therapy sessions.

- Recognizing inconsistencies in the data entered in one or more folders and identifying the personnel responsible for the update.

- Generating a report using one of the predefined templates.

- Displaying the necessary information using predefined query models.

- Selecting specific types of medical reports: ECG, EEG, laboratory tests, etc.

- Producing lists of patients, appointments, or reservations, etc., according to specific criteria.

- Printing reports and other types of generated documents.

- Transmitting data in a secure manner.

IC HEALTH

CERTIPORT®

4. Patient safety and clinical risk management

Prevention and control of risk

- Understanding the clinical risk management policies and the significance of the associated terms: damage, error, event, adverse event, an event prevented, sentinel event, clinical governance, and risk.

- Understanding how an adverse event occurrence in a complex system results from the combination of particular circumstances.

- Knowing the methods and tools for identifying risks: reports, meetings, visits, and focus groups, review of healthcare records, screening, and comments.

- Recognizing the key features of the analysis tools most widely used: root cause analysis (RCA), analysis of modes and effects of deficiencies, and clinical audits.

- Identifying the key features of the security plan.

- Appreciating the importance of ethics in the management of clinical risks.

- Understanding the importance of communication and the involvement of stakeholders.

Health records and professional liability

- Understanding the role of health records as a tool for analysis and risk prevention: medical records, informed consent, nursing documentation, integrated healthcare records, health records in general medicine and dentistry, and the hospital discharge record.

- Recognizing professional liability, including medical, legal, economic, and insurance aspects.

Technological risk

- Analyzing and evaluating the risk associated with the use of biomedical equipment technology.

5. Internet and professional updating in medicine

Use of tools and resources

- Knowing the main Web addresses of clinical trials, guideline databases, the Web sites of scientific congresses, and sites containing scientific and medical information.

- Understanding how to use the sites, tools, and Web applications in medicine, such as RSS feeds, podcasts, YouTube videos, wikis, blogs, and social networks.

Data bank and research

- Knowing how to use the main data bank in medicine: what a data bank is, subject/keyword designations, what the data bank contains, and when to use it. Knowing how to set up a search using logical operators and how to activate the alert.

- Finding information in the medical field: Google, Google Books, and Google Scholar.

- Finding pictures and movies that deal with medicine: Google Image Search, Google Maps, and Google Earth.