TESTPASSPORT

QUESTIONS D'ENTRAÎNEMENT

UN MEILLEUR ACCOMPAGNEMENT

https://www.testpassport.fr

Mises à jour gratuites pendant un an

Exam : **CHDA**

Title : AHIMA Certified Health Data Analyst

Version : DEMO

1.When does health information lose Protected Health Information (PHI) status under HIPAA?
A. When it is shared without consent
B. When it is encrypted
C. When it is deidentified
D. When it is archived
Answer: C
Explanation:
Health information loses its designation as Protected Health Information (PHI) under HIPAA when it is deidentified. Deidentification involves the process of removing or modifying personal identifiers from health information so that the individual to whom the information pertains cannot be readily identified. According to HIPAA regulations, there are two methods for deidentification: the safe harbor method and the expert determination method. In the safe harbor method, 18 specific types of identifiers must be removed, including names, geographical subdivisions smaller than a state, elements of dates, and any other unique identifying number, characteristic, or code. Once this information is stripped away, the data can no longer be linked to an individual, thereby losing its PHI status. Consequently, the data can be used for research and analysis without the constraints that apply to PHI, such as requiring patient consent. Deidentification is important because it allows for the utilization of health data for various purposes, including research and public health, while still protecting individual privacy. The other listed options do not lead to the loss of PHI status under HIPAA. For instance, sharing information without consent or simply archiving data does not alter its status as PHI, and encryption, while enhancing security, does not ensure that

2.When does medical information lose its Protected Health Information (PHI) status under HIPAA?
A. When shared between two healthcare providers
B. When it is deidentified
C. When a patient requests access
D. When it is stored in a secure database
Answer: B
Explanation:
Medical information loses its Protected Health Information (PHI) status under HIPAA when it is deidentified. Deidentification refers to the process of removing or altering personal identifiers from health information so that individuals cannot readily be identified. This can be achieved through either the removal of specific identifiers or by applying statistical methods to ensure that the data cannot be linked back to an individual. Once the process of deidentification is complete, the data is no longer considered PHI and falls outside the protections of HIPAA. This allows for the use of health data in research and public health without compromising patient privacy. In contrast, sharing medical information between healthcare providers keeps it within the realm of PHI, as it still identifies individuals and is related to their health condition. A patient requesting access to their own medical information does not remove its PHI status; rather, it provides patients with rights regarding their own data. Storing information in a secure database does not change the status of the data itself; it merely specifies how the data is being safeguarded, keeping it protected under HIPAA as long as it contains identifiable information.

3.What is the optimal relationship between strategic planning and strategic IM planning in a healthcare entity?

A. They are separate processes with no interaction
B. They are clearly related, and CIO involvement is crucial
C. IM planning should be done only after strategic planning
D. Strategic IM planning is outdated
Answer: B
Explanation:
The optimal relationship between strategic planning and strategic information management (IM) planning in a healthcare entity is that they are clearly related, with the involvement of the Chief Information Officer (CIO) being crucial. This relationship emphasizes the integration of information management strategies into the broader strategic goals of the organization. In a healthcare setting, strategic planning outlines the organization's long-term goals and the overall direction it aims to take. On the other hand, strategic IM planning focuses on how to effectively manage information systems and technology that will support those broader goals. The CIO plays a vital role in ensuring that the IM strategies align with the healthcare entity's strategic objectives, facilitating seamless information flow and decision-making processes. The involvement of the CIO is particularly important because they bring expertise in technology and data management, which are essential for implementing the strategic vision. By aligning the IM planning with overall strategic initiatives, healthcare entities can better utilize data and technology to enhance patient care, improve operational efficiencies, and achieve their strategic objectives. This collaborative approach leads to a more cohesive and informed planning process that ultimately benefits the organization as a whole.

4.What is a primary function of a database administrator?
A. Developing application software
B. Managing data quality
C. Conducting patient surveys
D. Training healthcare staff
Answer: B
Explanation:
Managing data quality is a primary function of a database administrator because it involves ensuring that data is accurate, consistent, and reliable for users. This responsibility is critical in maintaining the integrity of the database and ensuring that the data can support decision-making processes in healthcare environments. By monitoring and implementing data management practices, a database administrator safeguards the quality of the information stored in the database, enabling effective analysis and reporting. In contrast, developing application software typically falls under the purview of software developers or engineers, who focus on building and creating applications rather than managing the data within a database. Conducting patient surveys is a task more related to clinical staff or research teams who gather data for various purposes, such as quality improvement or patient satisfaction assessments, rather than database management. Training healthcare staff is usually done by educators or specialists within the healthcare organization, focusing on ensuring that staff can use the tools and resources effectively, not specifically related to the management of database systems.

5.What is the recommended step to ensure continuity of care when backloading data into a new clinical documentation system?
A. Data migration

B. Data backup
C. Data mapping
D. Data analytics
Answer: C
Explanation:
The recommended step to ensure continuity of care when backloading data into a new clinical documentation system is data mapping. This process involves understanding how data from the old system will correspond to the new system. By mapping data, healthcare organizations can ensure that crucial patient information is accurately transferred and appropriately placed within the new system's framework. Data mapping helps to identify the fields and data types in the original system and aligns them with the corresponding areas in the new system. Thus, it minimizes the risk of data loss or misplacement, which is vital for maintaining the integrity of patient records and ensuring that clinicians have access to complete and relevant information for ongoing patient care. Other processes like data migration and data backup are indeed important in the context of transferring and securing data, but they do not specifically address the alignment of data from the old system to the new one. Data analytics, while valuable for interpreting the data once implemented, does not play a direct role in the transfer process itself and ensuring that the continuity of care is maintained during the transition.