TESTPASSPORT

QUESTIONS D'ENTRAÎNEMENT

UN MEILLEUR ACCOMPAGNEMENT

https://www.testpassport.fr

Mises à jour gratuites pendant un an

Exam : **CHPS**

Title : AHIMA Certified in Healthcare Privacy and Security

Version : DEMO

1.The use of role-based access in healthcare is an example of which concept?
A. Data minimization
B. Privacy rule compliance
C. Access control
D. Information sharing policy
Answer: C
Explanation:
Role-based access in healthcare is fundamentally an example of access control. This approach involves granting permissions and access to information based on the specific roles of individuals within an organization. By implementing role-based access, healthcare institutions can ensure that employees, clinicians, and other personnel have access only to the data necessary for them to perform their job functions, thereby limiting exposure to sensitive information and reducing the risk of data breaches or unauthorized access. Access control mechanisms, such as role-based access, are crucial in maintaining the security and privacy of healthcare information. They help in enforcing data protection policies by allowing fine-tuned access management that aligns with job responsibilities. This method enhances compliance with privacy regulations by ensuring that individuals only see or interact with the information pertinent to their role, therefore reinforcing the organization's commitment to safeguarding patient data. While data minimization, privacy rule compliance, and information sharing policies are important components in the broader context of healthcare data management, they do not specifically characterize the systematic control of access that role-based access entails.

2.Which regulations outline how to implement policies and procedures for protecting card transactions?
A. Health Insurance Portability and Accountability Act
B. Payment Card Industry Data Security Standard (PCD DDS)
C. Federal Information Security Management Act
D. Gramm-Leach-Bliley Act
Answer: B
Explanation:
The Payment Card Industry Data Security Standard (PCI DSS) specifically outlines the requirements for organizations that handle card transactions, ensuring that they implement effective policies and procedures to protect cardholder data. This standard was developed to enhance security measures and prevent data breaches, providing a framework that includes encryption, network security, access control, monitoring, and testing methods to safeguard sensitive payment information. While the other options address various aspects of data protection and privacy in different contexts, they do not focus specifically on the protection of card transactions. The Health Insurance Portability and Accountability Act (HIPAA) pertains to the privacy and security of health information; the Federal Information Security Management Act (FISMA) relates to federal information systems; and the Gramm-Leach-Bliley Act focuses on financial institutions and the sharing of consumers' personal financial information. None of these regulations provide the comprehensive guidelines specifically tailored to managing and securing payment card transactions as thoroughly as PCI DSS does.

3.An independent physician in a hospital may enter into which agreement for sharing protected health information?
A. Partnership agreement

B. Joint venture agreement
C. Organized healthcare arrangement
D. Service agreement
Answer: C
Explanation:
The correct answer is the organized healthcare arrangement. This type of agreement facilitates the sharing of protected health information (PHI) among healthcare providers while ensuring compliance with privacy regulations, particularly the Health Insurance Portability and Accountability Act (HIPAA). In organized healthcare arrangements, entities may coordinate their healthcare activities, which can include the sharing of patient information for treatment, payment, or healthcare operations without violating confidentiality rules. This framework is essential for enabling collaboration in patient care while maintaining the necessary protections for sensitive information. Other agreements, such as partnership agreements or service agreements, generally do not inherently focus on the sharing of PHI and may not sufficiently address the regulatory requirements for privacy and security. Joint venture agreements, while potentially allowing for collaboration, may lack the specific intent and structure designed to protect PHI involved in organized healthcare arrangements.

4.What is one reason a covered entity may deny a request for an amendment of protected health information?
A. The amendment isn't justified
B. The information is not part of the designated record set
C. The patient did not provide identification
D. The amendment request was submitted late
Answer: B
Explanation:
A covered entity may deny a request for an amendment of protected health information if the information is not part of the designated record set. The designated record set includes the medical records and billing records about individuals maintained by or for a covered entity, as well as other records used to make decisions about individuals. If the information in question does not fall within this set, the covered entity is not obligated to amend it, since the right to request amendments only applies to information that is part of the designated record set. This ensures that the amendment process is confined to relevant and official records that impact patient care and rights. In contrast, justification for the amendment, patient identification, or the timing of the request are generally not standalone reasons for denial under the regulations governing records management and patients' rights concerning their health information.

5.For a data breach on March 2, 2016, when is the latest notification date to the Department of Health and Human Services?
A. March 15, 2016
B. April 15, 2016
C. May 1, 2016
D. June 1, 2016
Answer: C
Explanation:
The correct answer reflects the requirements set forth by the Health Insurance Portability and

Accountability Act (HIPAA) regarding the notification of data breaches. According to HIPAA guidelines, covered entities are required to notify the Department of Health and Human Services (HHS) no later than 60 days after the discovery of a breach. In this case, the breach occurred on March 2, 2016. Therefore, the latest date for notifying HHS would be calculated by adding 60 days to that date. This results in a deadline of May 1, 2016. Meeting this timeline is crucial for compliance with regulatory requirements regarding data privacy and security in the healthcare sector.