RHIT Domain 2 – Health Data Maintenance and Analysis Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **Which aspect of health records is most likely to require patient authorization for release?**

   A. Patient demographics

   B. Discharge summaries

   C. Psychotherapy notes

   D. Clinical lab results

2. **What should a supervisor do if an employee is printing unusually large quantities of patient records?**

   A. Reprimand the employee

   B. Fire the employee

   C. Determine what information was printed and why

   D. Revoke the employee's access privileges

3. **Under HIPAA, which of the following is not named as a covered entity?**

   A. Attending physician

   B. Healthcare clearinghouse

   C. Health plan

   D. Outsourced transcription company

4. **A home health agency plans to implement a computer system whereby its nurses document home care services on a laptop computer taken to the patient's home. What would be the best practice to protect laptop and network data from a virus introduced from an external device?**

   A. Biometrics

   B. Encryption

   C. Personal firewall software

   D. Session terminations

5. **Which aspect of health data management is improved through the use of data governance?**

   A. Patient engagement in treatment choices

   B. Reduction of data storage costs

   C. Data quality and compliance with regulations

   D. Automation of clinical workflows

6. Access to health records based on protected health information within a healthcare facility should be limited to employees who have what?

A. Legitimate need for access

B. Password

C. Report development program

D. Signed confidentiality agreement

7. Which are security safeguards that protect equipment, media, and facilities?

A. Administrative controls

B. Physical safeguards

C. Audit controls

D. Role based safeguards

8. Which document directs an individual to bring originals or copies of records to court?

A. Summons

B. Subpoena

C. Subpoena duces tecum

D. Deposition

9. In the context of HIPAA, what does PHI stand for?

A. Patient Health Information

B. Protected Health Information

C. Public Health Information

D. Privacy Health Information

10. To ensure relevancy, an organization's security policies and procedures should be reviewed at least:

A. Once every six months

B. Once a year

C. Every two years

D. Every five years

Answers

1. C
2. C
3. D
4. C
5. C
6. A
7. B
8. C
9. B
10. B

Explanations

1. Which aspect of health records is most likely to require patient authorization for release?

A. Patient demographics

B. Discharge summaries

C. Psychotherapy notes

D. Clinical lab results

The aspect of health records that most likely requires patient authorization for release is psychotherapy notes. This is due to the heightened sensitivity and confidentiality associated with mental health information. Psychotherapy notes contain detailed and personal information about a patient’s mental health, treatment strategies, and the therapist's observations or insights. As such, they are granted additional protections under laws such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. In contrast, other components of health records, such as patient demographics, discharge summaries, and clinical lab results, generally do not require specific patient consent for release. Patient demographics are basic identifying information that typically is considered public. Discharge summaries provide a clinical overview necessary for continuing care and may be shared with other healthcare providers without additional authorization. Clinical lab results are usually considered essential for medical treatment and can be accessed under general healthcare practices. Therefore, the need for authorization primarily pertains to psychotherapy notes due to their confidential nature.

2. What should a supervisor do if an employee is printing unusually large quantities of patient records?

A. Reprimand the employee

B. Fire the employee

C. Determine what information was printed and why

D. Revoke the employee's access privileges

Determining what information was printed and why is the most appropriate course of action in this scenario. This approach aligns with best practices in data governance, allowing the supervisor to gather context before jumping to conclusions. Understanding the reasoning behind the large print volume can uncover legitimate needs, such as preparing reports for patient care or fulfilling a requisition for information from another department.   This investigation is critical as it helps ensure that the actions are based on understanding rather than assumption, potentially addressing any genuine needs the employee might have. Additionally, it reflects a commitment to due process and accountability, which are essential in maintaining trust and a positive work environment. Taking other actions, such as reprimanding or firing the employee without understanding the situation, can lead to misunderstandings and can undermine morale. Similarly, revoking access privileges without insight into the reason could inhibit necessary functions and may be perceived as punitive rather than corrective. Hence, gathering detailed information allows supervisors to make informed decisions that uphold policies while also supporting their team.

3. Under HIPAA, which of the following is not named as a covered entity?

A. Attending physician

B. Healthcare clearinghouse

C. Health plan

D. Outsourced transcription company

In the context of HIPAA, covered entities are defined specifically to include healthcare providers, health plans, and healthcare clearinghouses that transmit health information in electronic form. The attending physician, healthcare clearinghouse, and health plan all fall under these definitions as they are directly involved in providing or processing healthcare information. An outsourced transcription company, however, does not qualify as a covered entity unless it is part of a larger covered entity's operations or if it directly handles protected health information (PHI) as a business associate. While these companies handle sensitive information, they typically work under contracts with covered entities and are considered business associates, thus they are not directly classified as covered entities in the same way. Understanding this distinction is vital in navigating HIPAA regulations, as covered entities have specific compliance obligations that do not extend to business associates. This clarity illustrates the roles and responsibilities surrounding patient data and the flow of information in the healthcare system.

4. A home health agency plans to implement a computer system whereby its nurses document home care services on a laptop computer taken to the patient's home. What would be the best practice to protect laptop and network data from a virus introduced from an external device?

A. Biometrics

B. Encryption

C. Personal firewall software

D. Session terminations

The best practice for protecting laptop and network data from a virus introduced from an external device is to use personal firewall software. A personal firewall serves as a barrier between the laptop and potential threats coming from outside sources, including external devices that could carry viruses or malware. It monitors incoming and outgoing network traffic and can block unauthorized access or potentially harmful connections, thereby providing an essential layer of defense. By implementing personal firewall software, the home health agency can ensure that any data transactions or connections made by the laptop while in a patient's home are secure, helping to protect sensitive health information. This is particularly important in a home health setting, where devices may frequently connect to different networks, increasing the risk of exposure to external threats. In the context of the other options, while biometrics and encryption are important for securing data, they primarily focus on user access and protecting data at rest or in transit rather than specifically addressing real-time threats from external devices. Session terminations are also useful but mainly deal with inactivity or timeout for user sessions rather than providing active protection against incoming threats.

5. **Which aspect of health data management is improved through the use of data governance?**

   A. Patient engagement in treatment choices

   B. Reduction of data storage costs

   C. Data quality and compliance with regulations

   D. Automation of clinical workflows

Data governance is essential for ensuring that health data is accurate, reliable, and compliant with relevant regulations. By implementing data governance frameworks, healthcare organizations establish clear policies and procedures for managing data throughout its lifecycle. This includes defining data standards, ensuring data integrity, and maintaining compliance with legal and regulatory requirements, such as HIPAA. Additionally, data governance promotes accountability and proper data stewardship, which are critical components in maintaining high-quality healthcare data. This structured approach helps identify and rectify issues related to data quality, such as inconsistencies or inaccuracies, and also ensures that data handling processes align with regulatory standards.   In contrast, while patient engagement, reduction of storage costs, and automation of clinical workflows are important aspects of health data management, they are not directly linked to the primary function of data governance. Data governance specifically targets the oversight of data quality and compliance, which ultimately supports the broader goals of health information management. This focus on quality and compliance contributes to improved patient outcomes and operational efficiencies within healthcare organizations.

6. **Access to health records based on protected health information within a healthcare facility should be limited to employees who have what?**

   A. Legitimate need for access

   B. Password

   C. Report development program

   D. Signed confidentiality agreement

Access to health records containing protected health information (PHI) within a healthcare facility is critically governed by rules designed to maintain patient privacy and ensure data security. The principle of "minimum necessary access" is crucial in healthcare settings, emphasizing that only those employees who have a legitimate need for access should be able to view patient records.   This legitimate need typically relates to the employee's job functions, such as clinical staff needing information to provide care, billing personnel requiring data for insurance claims, or administrative staff needing access for managing patient information. By restricting access based on these criteria, healthcare organizations can protect sensitive patient information from unauthorized release or misuse. While a password is essential for securing access to electronic systems, it does not alone justify access to health records unless there is a legitimate need. Similarly, while signed confidentiality agreements are important for ensuring that employees understand their responsibilities regarding patient data, the fundamental criterion for access remains the legitimate need. Therefore, having a legitimate need for access aligns with the principles of confidentiality and data security in healthcare environments.

7. Which are security safeguards that protect equipment, media, and facilities?

A. Administrative controls

B. Physical safeguards

C. Audit controls

D. Role based safeguards

The correct answer is physical safeguards. These are essential components of security measures designed to protect the physical aspects of information systems and health data. Physical safeguards include measures that secure equipment, media, and facilities from unauthorized access, natural disasters, and environmental hazards. Examples of physical safeguards are security locks, surveillance cameras, alarms, and secure server rooms that help safeguard physical assets from theft or damage. Understanding the role of physical safeguards is crucial in ensuring the overall security of health data management systems. Without robust physical security measures in place, sensitive information can be at risk of exposure or loss, emphasizing the need for a comprehensive security strategy that addresses all potential vulnerabilities related to infrastructure. Administrative controls, on the other hand, focus on policies, procedures, and practices for managing the overall security environment. Audit controls relate to monitoring and evaluating access and integrity of data systems, while role-based safeguards pertain to access controls based on the specific roles of individuals within an organization. These aspects are important, but they do not pertain directly to the protection of physical resources themselves.

8. Which document directs an individual to bring originals or copies of records to court?

A. Summons

B. Subpoena

C. Subpoena duces tecum

D. Deposition

The correct document that directs an individual to bring originals or copies of records to court is the subpoena duces tecum. This type of subpoena specifically requires a person to produce documents, records, or evidence in a legal proceeding. It is a legal order that compels the disclosure of pertinent records that may be relevant to a case, allowing for the examination of such materials as evidence in court. In contrast, a summons is primarily a document used to notify an individual that they are being sued or required to appear in court, but it does not require the production of documents. A general subpoena may require an individual to appear in court but does not specify the need to bring documents or records. On the other hand, a deposition is a sworn out-of-court testimony that is recorded for later use in court, but it does not inherently require the production of documents either. Thus, the specificity of the subpoena duces tecum in requiring the production of originals or copies of records makes it the correct choice in this context.

9. In the context of HIPAA, what does PHI stand for?

- A. Patient Health Information
- B. Protected Health Information
- C. Public Health Information
- D. Privacy Health Information

The term PHI stands for Protected Health Information, which is a key concept within the Health Insurance Portability and Accountability Act (HIPAA). PHI refers to any individually identifiable health information that is created, received, maintained, or transmitted by a covered entity or business associate. This includes details such as a patient's name, address, social security number, medical records, and any other information that can be used to identify an individual and is related to their health condition, healthcare provision, or payment for healthcare services. HIPAA establishes strict guidelines and regulations to ensure the privacy and security of this sensitive information. The classification as "protected" highlights the legal requirement to safeguard this data against unauthorized access and disclosure. Understanding PHI is crucial for healthcare professionals and organizations to comply with HIPAA regulations and to protect patients' rights regarding their health information.

10. To ensure relevancy, an organization's security policies and procedures should be reviewed at least:

- A. Once every six months
- B. Once a year
- C. Every two years
- D. Every five years

Reviewing an organization's security policies and procedures at least once a year aligns with best practices in risk management and compliance. This frequency is essential to ensure that the policies remain relevant to the evolving security landscape, emerging threats, and changes in organizational structure or operations. Annual reviews provide an opportunity to assess the effectiveness of existing security measures, make necessary updates, and ensure compliance with legal and regulatory requirements that may have changed over time. Additionally, considering the pace at which technology and cybersecurity threats evolve, annual reviews help organizations stay proactive rather than reactive. This frequency allows for timely updates that can mitigate risks associated with outdated or ineffective policies. Regular evaluations support continuous improvement in the organization's security posture, safeguarding sensitive data and maintaining stakeholder trust. In contrast, reviewing security policies at less frequent intervals, such as every two, five years, or even six months, may lead to lapses in security measures and heightened risk exposure during periods without updates. Annual reviews strike an appropriate balance between thoroughness and adaptability to changing circumstances in the security realm.