Certified in Healthcare Privacy and Security (CHPS) Practice (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **From which systems must an organization provide a copy of protected health information upon request?**

   A. Physical record systems only

   B. All electronic systems

   C. Only the EMR system

   D. Manual record systems

2. **Which HIPAA standard defines the process for granting access to protected health information?**

   A. Access control

   B. Access authorization

   C. Access management

   D. Information sharing policies

3. **If a data breach occurred on September 25, 2015, when must the hospital notify the Department of Health and Human Services at the latest?**

   A. January 2, 2016

   B. September 25, 2015

   C. March 31, 2016

   D. April 30, 2016

4. **What is the primary function of healthcare operations in relation to protected health information?**

   A. To disclose patient information to third parties

   B. To manage the business aspects of healthcare

   C. To conduct medical research

   D. To improve patient treatment outcomes

5. **Which factor needs to be identified during a breach investigation regarding PHI faxed to an unauthorized person?**

   A. The unauthorized person who discovered the PHI

   B. The identity of the PHI owner

   C. The extent of the disclosure

   D. The method of transmission of the PHI

6. What must be conducted when an organization experiences a data breach involving three or more unsuccessful log-in attempts?

A. Risk assessment

B. Behavioral analysis

C. Log-in monitoring policy review

D. Incident report generation

7. What documentation should a covered entity maintain after notifying individuals of a data breach?

A. A list of all individuals notified

B. A copy of the notification letter and the date of notification

C. All correspondence with law enforcement

D. Both A and B

8. Which of the following describes a method to monitor user access to a system?

A. Session timeout

B. Log-in monitoring

C. Data encryption

D. Access control list

9. What should a covered entity do if an authorization for disclosure is received without a signature date?

A. Process the request without the date

B. Deny the request and ask for the date of signature

C. Accept the request as valid

D. Request additional documentation

10. Which statement is true regarding the penalties for HIPAA violations?

A. The penalties have a single tier

B. All violations result in the same fine

C. Penalties are based on the intent behind the violation

D. Compliance is only monitored annually

Answers

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

Explanations

1. From which systems must an organization provide a copy of protected health information upon request?

A. Physical record systems only

B. All electronic systems

C. Only the EMR system

D. Manual record systems

The correct choice highlights that an organization must provide a copy of protected health information (PHI) from all electronic systems. This is in alignment with the regulations established by the Health Insurance Portability and Accountability Act (HIPAA), which mandates covered entities to provide individuals access to their PHI, regardless of the medium or format in which the information is maintained. Electronic health records and other digital platforms store significant amounts of health information, and individuals have the right to receive copies of their data in a format that meets their needs. The emphasis on electronic systems is important because they often contain the most comprehensive and up-to-date information regarding a patient's health history, treatment, and billing. In contrast, focusing solely on physical record systems or manual systems would neglect the wide array of data stored electronically, which is increasingly the standard for healthcare information management. The option related to the EMR system alone also narrows down the response incorrectly, as many organizations utilize a variety of electronic systems—such as health information exchanges and other digital applications—that may contain PHI. Thus, including all electronic systems ensures compliance with legal requirements and supports the patients' rights to access their health information conveniently and thoroughly.

2. Which HIPAA standard defines the process for granting access to protected health information?

A. Access control

B. Access authorization

C. Access management

D. Information sharing policies

The correct answer is access authorization. This standard outlines the specific processes and criteria for determining who is permitted to access protected health information (PHI) within a healthcare organization. By establishing access authorization protocols, healthcare entities ensure that only individuals with a legitimate need to know, such as healthcare providers and administrative staff, can access sensitive patient data. Access authorization plays a critical role in maintaining the confidentiality and security of PHI, as it directly addresses the need to safeguard this information from unauthorized access. Elements of access authorization include role-based access controls, user authentication methods, and the establishment of user privileges that align with the individual's job responsibilities. The other choices, while related to the topic of access control in healthcare, do not specifically define the formal process for granting access to PHI. Access control generally refers to the broader concept of restricting access to information, whereas access management could encompass the overall administration of user access rights but does not define the process itself. Information sharing policies guide how and when data may be shared but do not specifically address the individual access rights to PHI. Thus, access authorization is the standard that most directly aligns with the process of granting access to protected health information in a compliant manner.

3. If a data breach occurred on September 25, 2015, when must the hospital notify the Department of Health and Human Services at the latest?

A. January 2, 2016

B. September 25, 2015

C. March 31, 2016

D. April 30, 2016

The question tests understanding of how HIPAA breach notifications to HHS differ by the number of individuals affected. If a breach affects 500 or more people, the entity must notify HHS within 60 days after discovery. But when the breach involves fewer than 500 individuals, the rule requires an annual notification/report to HHS, not a 60-day notice. Since the breach happened on September 25, 2015 and involves fewer than 500 people, the required action is an annual report to HHS due the following year, by the end of the first quarter. That means no later than March 31, 2016. This is why March 31, 2016 is the latest acceptable date. (Note: notification to affected individuals is a separate requirement and would occur within 60 days of discovery, independent of the HHS reporting deadline.)

4. What is the primary function of healthcare operations in relation to protected health information?

A. To disclose patient information to third parties

B. To manage the business aspects of healthcare

C. To conduct medical research

D. To improve patient treatment outcomes

The primary function of healthcare operations in relation to protected health information is to manage the business aspects of healthcare. This involves overseeing a variety of administrative functions essential for healthcare delivery, such as billing, claims processing, financial management, and other operational activities. Effective management of these operations ensures that healthcare organizations can run smoothly and comply with regulations concerning the use and protection of protected health information (PHI). In managing these business aspects, healthcare operations professionals are responsible for ensuring that PHI is handled appropriately and securely while facilitating necessary administrative tasks. They play a critical role in maintaining the integrity and confidentiality of patient information, ultimately supporting the healthcare organization's overall mission and compliance with legal requirements, such as HIPAA. Other options may involve aspects of healthcare but do not define the primary function of healthcare operations in relation to PHI. Disclosing patient information to third parties must be done within legal and ethical guidelines, emphasizing the need for proper procedures rather than serving as a central purpose. Conducting medical research, while important, typically falls under different operational areas such as research compliance and ethics, not general healthcare operations. Likewise, improving patient treatment outcomes is a goal of healthcare in general but does not specifically align with the operational management of PHI.

5. Which factor needs to be identified during a breach investigation regarding PHI faxed to an unauthorized person?

A. The unauthorized person who discovered the PHI

B. The identity of the PHI owner

C. The extent of the disclosure

D. The method of transmission of the PHI

Identifying the unauthorized person who received the protected health information (PHI) is crucial during a breach investigation as it directly relates to the security and privacy incident's impact. Understanding who received the PHI can guide the response and mitigation strategies, including notifying affected individuals and relevant authorities as required by laws such as HIPAA. This identification helps the organization understand the breach's scope—the potential risk of identity theft or further dissemination of the information. Additionally, it can inform the necessary legal and compliance steps, including any required reporting to regulatory bodies. Considering the other factors, while the identity of the PHI owner, the extent of the disclosure, and the method of transmission are all important to the investigation, they do not specifically address who constitutes the unauthorized recipient. The urgency of notifying both the affected parties and regulatory bodies hinges significantly on knowing the recipient's identity and their capability or intent concerning the disclosed information.

6. What must be conducted when an organization experiences a data breach involving three or more unsuccessful log-in attempts?

A. Risk assessment

B. Behavioral analysis

C. Log-in monitoring policy review

D. Incident report generation

The correct answer pertains to the necessity of reviewing the log-in monitoring policy after an organization experiences a data breach indicating multiple unsuccessful log-in attempts. This situation signals a potential unauthorized access attempt, making it crucial for the organization to assess and refine its policies and procedures related to user authentication. Conducting a review of the log-in monitoring policy allows the organization to identify weaknesses, enhance security protocols, and ensure there are appropriate deterrents and responses in place to prevent future breaches. This may involve analyzing how unsuccessful log-in attempts are tracked, determining thresholds for action, and improving alerts for suspicious activities. The goal is to understand how the current policy may need to evolve to respond effectively to potential vulnerabilities. In contrast, while a risk assessment is an important aspect of overall security management, it is a broader analysis that may take time and resources beyond the immediate need for a policy review. Behavioral analysis focuses on examining user behavior over time rather than addressing a specific incident of failed log-ins. Incident report generation, while necessary for documenting the breach, serves a different purpose and does not immediately contribute to preventing future occurrences as effectively as a policy review would.

7. What documentation should a covered entity maintain after notifying individuals of a data breach?

A. A list of all individuals notified

B. A copy of the notification letter and the date of notification

C. All correspondence with law enforcement

D. Both A and B

Maintaining a list of all individuals notified and a copy of the notification letter, along with the date of notification, is crucial for a covered entity following a data breach. Documenting the individuals who were notified ensures that the entity has a clear record of compliance with legal obligations, as it confirms that all affected parties were informed appropriately and allows for accountability in the breach notification process. In addition, keeping a copy of the notification letter serves as a formal record of what information was provided to the individuals, which is vital for transparency and can also help in assessing the effectiveness of the communication. Recording the date of notification helps track the timeline related to the breach and can be important if there are inquiries or investigations by regulators or affected individuals. The combination of these records provides a comprehensive approach to documenting the entity's response to the breach, fulfilling both legal requirements and supporting effective breach management practices. This documentation can also be useful in future audits and assessments, ensuring that the entity can demonstrate adherence to privacy and security regulations.

8. Which of the following describes a method to monitor user access to a system?

A. Session timeout

B. Log-in monitoring

C. Data encryption

D. Access control list

Log-in monitoring is an effective method to track and oversee user access to a system. This involves keeping records of login attempts, which can include successful and failed logins, the duration of sessions, and the activities performed while logged in. By analyzing this data, organizations can identify unusual or suspicious access patterns, helping to detect unauthorized access or potential security breaches. While session timeout contributes to security by automatically logging users out after a period of inactivity, it does not directly monitor user access in the same way log-in monitoring does. Data encryption is focused on protecting data confidentiality and integrity, rather than tracking user activity. An access control list is essential for determining which users or systems can access specific resources but does not provide a means of monitoring user behavior. Thus, log-in monitoring stands out as the most appropriate method for monitoring user access to a system.

9. What should a covered entity do if an authorization for disclosure is received without a signature date?

A. Process the request without the date

B. Deny the request and ask for the date of signature

C. Accept the request as valid

D. Request additional documentation

In a situation where an authorization for disclosure is received without a signature date, the most appropriate action for a covered entity is to deny the request and ask for the date of the signature. This is because a signature date is critical to the validity of the authorization; it establishes the timeframe during which the authorization is applicable. Without this date, it cannot be determined if the authorization is current or if it has expired, which could lead to unauthorized disclosure of protected health information. Moreover, regulations such as the Health Insurance Portability and Accountability Act (HIPAA) emphasize the importance of clear and valid authorizations for the protection of patient privacy. Ensuring that all components, including the date, are complete is essential in compliance with these regulations. Accepting an authorization without a signature date could expose the covered entity to legal risks or improper disclosure of sensitive health information. Thus, requesting the date of the signature is aligned with best practices in health information management and legal compliance.

10. Which statement is true regarding the penalties for HIPAA violations?

A. The penalties have a single tier

B. All violations result in the same fine

C. Penalties are based on the intent behind the violation

D. Compliance is only monitored annually

The statement about penalties for HIPAA violations being based on the intent behind the violation is accurate because the Health Insurance Portability and Accountability Act (HIPAA) establishes a tiered system for penalties. This system considers factors such as the nature and purpose of the violated HIPAA rule, the circumstances of the violation, and the intention of the covered entity or business associate involved. Under this tiered approach, violations are categorized into different levels, ranging from unknowing violations, where the offender didn't know they were violating HIPAA, to willful neglect, where there is a conscious disregard for the requirements. The higher the intent or the more egregious the violation, the stiffer the penalties can be. This allows the enforcement agencies to impose fines that reflect the severity of the violation and the behavior of the violators, thereby promoting compliance with HIPAA regulations. In contrast, a single tier for penalties would suggest a lack of differentiation based on the nature of violations, and a uniform fine for all violations would not adequately address the varying degrees of severity and intent. Furthermore, compliance monitoring does not occur only on an annual basis; it can be ongoing, with investigations triggered by reported incidents or changes in compliance status. Thus, the focus on intent effectively encourages

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://chps.examzify.com

We wish you the very best on your exam journey. You've got this!