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. **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

2. **The HIPAA Security Rule allows flexibility with implementation based on reasonableness and appropriateness safeguards. This means that covered entities can:**

   A. Implement based on organizational assessment

   B. Implement without any assessment

   C. Follow strict national standards only

   D. Select any method they prefer

3. **A policy detailing permissible functions performed on computers within an organization is an example of what?**

   A. Privacy policy

   B. Data handling agreement

   C. Workstation use

   D. IT security policy

4. **What is the 'date of discovery' in the context of a breach?**

   A. The date when individuals are notified

   B. The first report of the breach

   C. The date the organization knew about the improper use of information

   D. The date the breach risk assessment is completed

5. **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

6. 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

7. 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

8. What is the term for the process that restores critical data as quickly as possible after a disruptive event?

A. Data recovery plan

B. Business continuity

C. Disaster recovery mode

D. Incident response

9. Which organization is responsible for maintaining and issuing public key certificates used in encryption?

A. Security Exchange Commission

B. Certificate authorities

C. Data Protection Agency

D. Privacy Board

10. What is defined as a facility security plan?

A. A new policy protecting the physical space of clinics

B. A plan for employee training on data privacy

C. A strategic initiative for data encryption

D. A risk management approach for patient data

Answers

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

Explanations

1. 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.

2. The HIPAA Security Rule allows flexibility with implementation based on reasonableness and appropriateness safeguards. This means that covered entities can:

A. Implement based on organizational assessment

B. Implement without any assessment

C. Follow strict national standards only

D. Select any method they prefer

The HIPAA Security Rule indeed allows covered entities to implement safeguards based on what is reasonable and appropriate for their specific circumstances. This flexibility is crucial because each covered entity has different resources, types of data, and levels of risk. By allowing implementation based on an organizational assessment, covered entities can evaluate their own unique environments, risks, and vulnerabilities, and then tailor their security measures accordingly. This process involves analyzing the operational needs, the type and volume of electronic protected health information (ePHI) managed, and assessing potential threats to their data security. As a result, organizations can adopt security controls that best fit their situation rather than adhering to a one-size-fits-all approach. The other choices indicate a more rigid or less customized approach to implementation, which does not align with the intent of the HIPAA Security Rule that aims to provide flexibility while still ensuring the protection of sensitive health information.

3. A policy detailing permissible functions performed on computers within an organization is an example of what?

A. Privacy policy

B. Data handling agreement

C. Workstation use

D. IT security policy

The correct choice, "Workstation use," pertains specifically to guidelines and rules regarding how computers and technology are to be utilized within an organization. This policy typically outlines permissible actions related to the use of workstations, including what applications can be installed, how data should be handled, and the expectations for secure behavior while using these devices. Such policies are essential to maintain the integrity and security of organizational data. Workstation use policies focus primarily on the operational aspect of computers, ensuring that employees understand their responsibilities when interacting with technology in ways that could impact organizational security and data privacy. This guidance is crucial as it helps protect sensitive information, mitigate risks associated with internal and external threats, and ensure compliance with relevant regulations.

4. What is the 'date of discovery' in the context of a breach?

A. The date when individuals are notified

B. The first report of the breach

C. The date the organization knew about the improper use of information

D. The date the breach risk assessment is completed

The 'date of discovery' in the context of a breach refers to the point at which an organization becomes aware of the unauthorized access or use of protected health information. This date is crucial because it initiates the organization's obligations under various regulations, such as the Health Insurance Portability and Accountability Act (HIPAA). Upon discovery, an organization must assess the breach's severity, determine the risk posed to individuals, and proceed with necessary notifications and remediation steps. Recognizing when improper use of information was discovered is vital for compliance and for protecting affected individuals' rights. Understanding this date can affect timelines for notifying individuals and authorities, the assessment of the breach's impact, and mitigating further risks. Inadequate knowledge of the other options shows why they do not represent the 'date of discovery.' For example, while notification may occur after the discovery, it does not represent the initial awareness of the breach itself. Additionally, the first report of the breach may not coincide with the organization's internal awareness, and completing a breach risk assessment occurs after the breach has been discovered and does not determine the actual date of discovery.

5. 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.

6. 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

7. 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

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.

8. What is the term for the process that restores critical data as quickly as possible after a disruptive event?

A. Data recovery plan

B. Business continuity

C. Disaster recovery mode

D. Incident response

The correct term for the process that focuses specifically on restoring critical data as quickly as possible after a disruptive event is known as disaster recovery mode. This term encapsulates the strategies and actions taken to resume operations and recover lost data following incidents such as natural disasters, cyberattacks, or hardware failures. Disaster recovery involves a defined set of procedures that ensure data integrity and availability, enabling an organization to return to its normal functioning with minimal downtime. This focus on quick data restoration is crucial in healthcare settings, where timely access to patient information is vital in maintaining care quality and compliance with regulations. Disaster recovery plans often include backup data storage systems, failover services, and restoration processes to minimize the impact of disruptions. In contrast, while a data recovery plan could be a component of the disaster recovery strategy focused on retrieving lost or corrupted data, it does not fully encompass the overall response to a disaster as disaster recovery mode does. Business continuity is a broader term that includes maintaining operations during a disruption rather than just focusing on data restoration. Incident response pertains more to the immediate actions taken during and shortly after a security incident to limit damage and secure systems, which is not exclusively about data recovery.

9. Which organization is responsible for maintaining and issuing public key certificates used in encryption?

A. Security Exchange Commission

B. Certificate authorities

C. Data Protection Agency

D. Privacy Board

The organization responsible for maintaining and issuing public key certificates used in encryption is known as Certificate authorities. These certificate authorities play a critical role in the Public Key Infrastructure (PKI), which is essential for secure communications over networks, particularly the internet. Certificate authorities validate the identity of entities (like individuals, organizations, or devices) before issuing digital certificates, which include public keys. These certificates help ensure that the public keys belong to the entity that claims to own them, enabling secure and encrypted communication. Because these certificates allow users to verify identities and establish trust in digital transactions, certificate authorities are integral to protecting sensitive information against unauthorized access during data transmission. The other organizations mentioned have different roles that do not involve the management of public key certificates. For example, the Securities and Exchange Commission focuses on regulating securities markets and protecting investors, while Data Protection Agencies oversee compliance with data protection laws and regulations. Privacy Boards generally review and advise on privacy-related matters within organizations but not specifically on encryption or public key certificates.

10. What is defined as a facility security plan?

A. A new policy protecting the physical space of clinics

B. A plan for employee training on data privacy

C. A strategic initiative for data encryption

D. A risk management approach for patient data

A facility security plan is defined as a comprehensive strategy that outlines the measures and policies designed to protect the physical space of clinics or healthcare facilities. This plan includes protocols for access control, surveillance, emergency response, and the overall physical security of the environment where healthcare services are delivered. It is focused on ensuring the safety and security of both patients and staff, as well as the protection of physical assets and sensitive data from unauthorized access or threats. While policies related to employee training on data privacy, initiatives for data encryption, and risk management approaches for patient data are all vital aspects of a healthcare organization's overall security strategy, they pertain more to information security and data management rather than directly addressing the physical space and access control measures specific to a facility. The facility security plan is crucial for establishing a safe and secure environment within healthcare settings.

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!