CERTIFIED IN HEALTHCARE PRIVACY AND SECURITY (CHPS) PRACTICE (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://chps.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

Table of Contents

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. 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

2. 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

3. If a USB drive containing sensitive patient information is encrypted, should a breach investigation be conducted?

A. Yes, because there is a risk of loss

B. No, the data is secure since the USB was encrypted

C. Yes, since it contains personal health information

D. No, if no patient data was accessed

4. What is typically included in a breach investigation?

A. Personal interviews with offenders

B. A review of all access logs

C. An assessment of whether the information was exfiltrated

D. All internal policies

5. What is one of the key purposes of the HIPAA Privacy Rule?

A. To ensure quicker delivery of healthcare services

B. To protect sensitive patient health information

C. To improve the efficiency of healthcare billing processes

D. To limit healthcare access to affordable providers

SAMPLE

6. What document outlines procedures for accessing facilities to support lost data recovery?

A. Business continuity plan

B. Contingency plan

C. Emergency response plan

D. Data security plan

7. What is one of the essential requirements for ensuring the security of protected health information?

A. Data encryption

B. Weekly team meetings

C. Marketing consent

D. External audits

8. What is required for a covered entity to disclose a patient's health information for marketing purposes?

A. A signed authorization from the patient

B. An oral agreement

C. A verbal approval

D. A written notice

9. What must be obtained by a healthcare organization when promoting a vehicle insurance product to a member?

A. Patient's consent

B. Authorization for disclosure for marketing purposes

C. Written notice of communication

D. Approval from the insurance board

10. What type of vendor is considered a business associate?

A. Data conversion consultant

B. Direct healthcare provider

C. Office supply vendor

D. Insurance agent

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. 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

2. 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.)

SAMPLE

3. If a USB drive containing sensitive patient information is encrypted, should a breach investigation be conducted?

A. Yes, because there is a risk of loss

B. No, the data is secure since the USB was encrypted

C. Yes, since it contains personal health information

D. No, if no patient data was accessed

The belief that a breach investigation is not necessary when a USB drive is encrypted stems from the understanding that encryption serves as a protective measure for sensitive information. When data is encrypted, it becomes unreadable without the appropriate decryption key, significantly reducing the risk of unauthorized access to the information. Thus, if a USB drive containing sensitive patient information is lost or stolen, the encrypted status indicates that even if the physical device falls into the wrong hands, the data contained within it remains secure, as it cannot be accessed without the key. However, this perspective may overlook the importance of breach investigation protocols. Conducting a breach investigation, regardless of the encryption, can provide insight into the circumstances surrounding the loss of the device and assess any total risk to patient privacy or potential data breach incidents. Understanding why the device was lost, how to prevent future occurrences, and confirming that no unauthorized access occurred are critical components of an effective information security program. The distinction lies in recognizing that while encryption is a strong safeguard, it does not entirely eliminate the need for examining the circumstances of a potential breach to ensure all relevant protocols and protective measures are effectively in place. Exploring these elements is paramount in maintaining the integrity of patient privacy and security standards within healthcare settings.

4. What is typically included in a breach investigation?

A. Personal interviews with offenders

B. A review of all access logs

C. An assessment of whether the information was exfiltrated

D. All internal policies

In a breach investigation, assessing whether the information was exfiltrated is a critical component. This process involves determining if sensitive or protected data has been accessed, copied, or transferred out of the organization's systems without authorization. This assessment is crucial for understanding the scope of the breach, the potential impact on affected individuals, and the necessary steps for remediation. By establishing whether data was exfiltrated, organizations can also begin to address potential vulnerabilities and work towards improving security measures to prevent future breaches. It also informs stakeholders and regulatory bodies about the nature of the incident, which is essential for compliance and transparency. While personal interviews, reviews of access logs, and evaluations of internal policies are relevant in a broader investigation context, they are not as directly critical as the assessment of data exfiltration when it comes to the core objectives of understanding the breach's consequences and mitigating any further risks.

SAMPLE

5. What is one of the key purposes of the HIPAA Privacy Rule?

A. To ensure quicker delivery of healthcare services

B. To protect sensitive patient health information

C. To improve the efficiency of healthcare billing processes

D. To limit healthcare access to affordable providers

One of the key purposes of the HIPAA Privacy Rule is to protect sensitive patient health information. The rule establishes national standards for the protection of certain health information, particularly concerning how such data is managed, shared, and communicated. It aims to ensure that individuals' health information is kept confidential and secure, providing patients with privacy rights regarding their own health data. This includes regulating who may access or disclose health information and under what circumstances. By focusing on the privacy and protection of health information, the HIPAA Privacy Rule plays a critical role in fostering trust between patients and healthcare providers, which is foundational in delivering quality healthcare.

6. What document outlines procedures for accessing facilities to support lost data recovery?

A. Business continuity plan

B. Contingency plan

C. Emergency response plan

D. Data security plan

The correct choice is the contingency plan, as it specifically outlines procedures and actions to be taken in response to unexpected events, such as data loss. A contingency plan typically includes strategies for recovering lost data, ensuring business operations can continue with minimal disruption. It provides guidance on how to access the necessary facilities and resources to support recovery efforts and restore normal operations. Business continuity plans focus on maintaining essential functions during and after a disaster but do not provide specific procedures for data recovery. While an emergency response plan deals with immediate responses to an emergency situation, it may not delve into the specifics of data recovery and facility access. The data security plan primarily addresses the protections and measures in place to safeguard against data breaches but is not centered on recovery procedures following data loss. Therefore, a contingency plan is the most appropriate document for detailing the necessary procedures to access facilities to recover lost data.

SAMPLE

7. What is one of the essential requirements for ensuring the security of protected health information?

A. Data encryption

B. Weekly team meetings

C. Marketing consent

D. External audits

Data encryption is a fundamental requirement for ensuring the security of protected health information (PHI). The process of encryption transforms data into a secure format that can only be read or processed after decryption, thereby protecting sensitive health information from unauthorized access. This is particularly vital in healthcare, where the confidentiality and integrity of patient information are paramount. Effective encryption acts as a safeguard in various scenarios, including data breaches and cyberattacks, as it renders the data unreadable to anyone who does not possess the proper encryption keys. While other options may contribute to the overall framework of security management within healthcare organizations, they do not specifically address the core need for protecting the confidentiality of PHI as directly as data encryption does. Weekly team meetings may promote awareness and collaboration but do not protect data in themselves. Marketing consent pertains to the use of patient information for promotional purposes and is not strictly related to data security. External audits can help assess compliance and identify vulnerabilities, but without robust data encryption, the underlying risk to PHI remains significant. Thus, encryption is recognized as a critical practice to ensure the security of healthcare data.

8. What is required for a covered entity to disclose a patient's health information for marketing purposes?

A. A signed authorization from the patient

B. An oral agreement

C. A verbal approval

D. A written notice

To disclose a patient's health information for marketing purposes, a covered entity is required to obtain a signed authorization from the patient. This requirement is in place to ensure that patients have control over their personal health information and are fully aware of how it might be used or disclosed, particularly for marketing initiatives that are not directly related to their health care. The signed authorization must include specific information regarding the type of information that will be shared and the purposes for the disclosure, ensuring transparency and respect for patient privacy rights. In contrast, options that involve oral agreements or verbal approvals do not provide a sufficient level of assurance and accountability, as they lack the formal documentation necessary to demonstrate consent. A written notice, while important for patient information, does not serve as a legitimate way to obtain consent for marketing-related disclosures. Hence, the requirement for a signed authorization places patients in a position of authority over their health information in marketing contexts.

SAMPLE

9. What must be obtained by a healthcare organization when promoting a vehicle insurance product to a member?

A. Patient's consent

B. Authorization for disclosure for marketing purposes

C. Written notice of communication

D. Approval from the insurance board

When a healthcare organization promotes a vehicle insurance product to a member, it is essential to obtain authorization for disclosure for marketing purposes. This requirement stems from regulations such as the Health Insurance Portability and Accountability Act (HIPAA), which governs how protected health information (PHI) can be used and disclosed, particularly for marketing initiatives. In this context, since promoting a vehicle insurance product is considered a marketing activity, explicit authorization is necessary to disclose any PHI to third parties involved in the marketing process. Unlike general patient consent, which may be assumed for treatment and healthcare operations, the use of PHI for marketing requires specific, informed consent from the patient. This ensures that individuals retain control over their personal health information and can make informed choices about how it is used in contexts outside of their direct care. Additional options mention various aspects of communication or approval processes that do not address the specific regulatory requirement for marketing, emphasizing the importance of obtaining proper authorization directly related to the marketing of products.

10. What type of vendor is considered a business associate?

A. Data conversion consultant

B. Direct healthcare provider

C. Office supply vendor

D. Insurance agent

A business associate is defined under the Health Insurance Portability and Accountability Act (HIPAA) as a person or entity that performs certain functions or activities on behalf of a covered entity that involves the use or disclosure of protected health information (PHI). In this context, a data conversion consultant fits the criteria as they likely handle PHI during the process of converting data to different formats, ensuring compliance with various regulations along the way. Vendors that do not handle PHI in a way that involves access, use, or disclosure in alignment with the definitions of a business associate are not classified as such. For example, direct healthcare providers are covered entities themselves and not considered business associates because they directly provide care to patients and are governed under HIPAA in a different manner. Similarly, an office supply vendor does not typically access or manage PHI in the course of providing supplies and services. Lastly, an insurance agent may facilitate insurance transactions but usually does not manage PHI directly and is bound by different privacy requirements in their role.

SAMPLE

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!

SAMPLE