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

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

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. What is the main purpose of HIPAA regulations regarding data breaches?

A. To maintain patient privacy and security

B. To enhance data storage techniques

C. To prevent electronic health records from being shared

D. To reduce healthcare costs

2. What is the primary responsibility of a privacy officer in a healthcare entity?

A. To conduct financial audits

B. To ensure compliance with privacy laws

C. To manage patient relations

D. To oversee insurance claims

3. 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

4. What do we call a payment from a drug company to promote a new medication for acne?

A. Indirect

B. Direct

C. Confidential

D. Authorized

5. 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

SAMPLE

6. If a health plan receives a request for confidential communication due to endangerment concerns, what must the health plan do?

A. Ignore the request

B. Permit and accommodate reasonable requests for confidential communication

C. Request proof of endangerment

D. Allow limited communication only

7. Which group was granted authority to bring civil actions against healthcare organizations and business associates based on alleged HIPAA violations?

A. Federal Trade Commission

B. State attorney general

C. Department of Health and Human Services

D. Local health departments

8. If a patient has made multiple requests for accounting-of-disclosures reports, which statement is correct regarding the fees charged?

A. The CE can charge a fee for all requests

B. No fees can be charged regardless of the number of requests

C. The CE may charge a reasonable, cost-based fee for subsequent requests

D. Fees can only be charged if the requests exceed five in a year

9. What consequence might occur if a covered entity is found to have acted with reasonable cause in failing to comply with HIPAA?

A. They will face immediate penalties

B. They will be required to undergo additional training

C. They may avoid severe penalties

D. They will be put on probation

10. Which two identifiers are part of both a limited data set and deidentified information?

A. Telephone number and email address

B. Geographic subdivision and elements of date

C. Full address and birthdate

D. Social security number and medical record number

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the main purpose of HIPAA regulations regarding data breaches?

A. To maintain patient privacy and security

B. To enhance data storage techniques

C. To prevent electronic health records from being shared

D. To reduce healthcare costs

The primary goal of HIPAA (Health Insurance Portability and Accountability Act) regulations is indeed to maintain patient privacy and security. This legislation was enacted to protect sensitive patient information from being disclosed without the patient's consent or knowledge. By implementing strict guidelines regarding how healthcare providers, insurers, and their business associates handle and share protected health information (PHI), HIPAA aims to safeguard against data breaches and unauthorized access. Keeping patient data secure is essential not only for maintaining patient trust but also for ensuring compliance with legal standards. The regulations set forth by HIPAA require organizations to employ various safeguards, including administrative, physical, and technical protections, to mitigate the risk of data breaches. This foundational aspect of HIPAA reflects the broader objective of protecting individual privacy rights in healthcare settings, ultimately fostering a safer environment for the handling of personal health information.

2. What is the primary responsibility of a privacy officer in a healthcare entity?

A. To conduct financial audits

B. To ensure compliance with privacy laws

C. To manage patient relations

D. To oversee insurance claims

The primary responsibility of a privacy officer in a healthcare entity is to ensure compliance with privacy laws. This role is crucial because privacy officers are tasked with developing, implementing, and overseeing policies and procedures that protect sensitive patient information, particularly in adherence to regulations such as the Health Insurance Portability and Accountability Act (HIPAA). They work to safeguard patient data from unauthorized access, breaches, and potential misuse, thereby promoting trust and integrity within the healthcare system. While other responsibilities, such as managing patient relations or overseeing insurance claims, are important in the overall operations of a healthcare organization, they do not specifically focus on the complexities and requirements of privacy regulations. Additionally, financial audits are related to the fiscal health of the entity but fall outside the privacy officer's core mandates. The privacy officer's work is central to ensuring that the organization complies with legal standards for protecting patient privacy and handling sensitive health information responsibly.

SAMPLE

3. 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

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.

4. What do we call a payment from a drug company to promote a new medication for acne?

A. Indirect

B. Direct

C. Confidential

D. Authorized

The correct answer is "Direct." This term is used to describe a payment that is made explicitly for the purpose of promoting a product or service, such as a medication. In the context of pharmaceutical companies, when a drug company provides financial support or payments directly to healthcare professionals to promote a new medication, it is classified as a direct payment. This involvement can include fees for speaking engagements, consulting, or sponsorship of educational events focused on the medication. Recognizing the nature of direct payments is crucial in understanding the dynamics of healthcare marketing and the potential impact on prescribing practices. This also ties into regulations and ethical considerations surrounding transparency and potential conflicts of interest in healthcare settings. Understanding this classification helps in grasping the broader implications of financial relationships between healthcare providers and pharmaceutical companies.

SAMPLE

5. 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.

6. If a health plan receives a request for confidential communication due to endangerment concerns, what must the health plan do?

A. Ignore the request

B. Permit and accommodate reasonable requests for confidential communication

C. Request proof of endangerment

D. Allow limited communication only

Permitting and accommodating reasonable requests for confidential communication is fundamental for health plans when they receive such requests due to endangerment concerns. This aligns with regulations and ethical practices that prioritize patient safety and privacy. When an individual indicates that they feel endangered, often due to domestic violence or similar circumstances, accommodating their request can help ensure their physical safety and emotional well-being. Health plans have a responsibility to take these concerns seriously and to implement appropriate safeguards. By allowing confidential communications, they enable individuals to maintain privacy regarding sensitive health information, which is critical in situations where information could be used against them. This approach demonstrates a commitment to protecting the individual's rights and ensuring they have a supportive environment in which they can seek necessary medical care without fear of further endangerment. While options like ignoring the request or requesting proof of endangerment could contribute to further distress for the individual, accommodating reasonable requests helps to build trust and ensures compliance with legal and ethical standards that aim to protect vulnerable populations. This reflects an understanding of the complexities involved in cases of potential endangerment and reinforces the importance of patient-centered care in health plan operations.

SAMPLE

7. Which group was granted authority to bring civil actions against healthcare organizations and business associates based on alleged HIPAA violations?

A. Federal Trade Commission

B. State attorney general

C. Department of Health and Human Services

D. Local health departments

The group granted authority to bring civil actions against healthcare organizations and business associates based on alleged HIPAA violations is the state attorney general. This authority is rooted in the Health Information Technology for Economic and Clinical Health (HITECH) Act, which empowers state attorneys general to enforce HIPAA regulations in their jurisdictions. They can investigate suspected violations and file lawsuits on behalf of the state and its residents when there is a belief that HIPAA has been violated, particularly if the violation affects the privacy and security of personal health information. This role is crucial because it enhances the enforcement of HIPAA at the state level, allowing local authorities to address violations that may not be handled directly by federal entities. While federal agencies like the Department of Health and Human Services oversee compliance and can initiate actions for violations, state attorneys general can act independently in enforcing HIPAA, adding an essential layer of protection for consumers. In this context, other groups mentioned, like the Federal Trade Commission, which focuses more on trade practices, the Department of Health and Human Services, which has oversight over HIPAA compliance but does not file civil actions, and local health departments, which typically deal with public health issues rather than enforcement of HIPAA, do not have the same authority to bring civil actions for HIP

8. If a patient has made multiple requests for accounting-of-disclosures reports, which statement is correct regarding the fees charged?

A. The CE can charge a fee for all requests

B. No fees can be charged regardless of the number of requests

C. The CE may charge a reasonable, cost-based fee for subsequent requests

D. Fees can only be charged if the requests exceed five in a year

The correct statement regarding fees charged for accounting-of-disclosures requests is that the covered entity (CE) may charge a reasonable, cost-based fee for subsequent requests. This provision is in accordance with the regulations under the Health Insurance Portability and Accountability Act (HIPAA), which allows covered entities to charge for the cost of producing and transmitting the requested information. The basis for charging a reasonable fee is intended to cover the administrative costs incurred in providing the accounting-of-disclosures reports beyond the first request. This approach recognizes that while patients have the right to access information about disclosures of their health information, the entities also incur expenses in fulfilling these requests. Therefore, if a patient exceeds a certain number of requests, charging a fee ensures a balance between patient rights and the financial viability of the healthcare entity. This fee should not be punitive and must be related directly to the actual costs involved in preparing the reports. This reasoning aligns with the regulatory framework that encourages transparency and access while also considering the operational realities faced by healthcare organizations when handling repeated requests from patients.

SAMPLE

9. What consequence might occur if a covered entity is found to have acted with reasonable cause in failing to comply with HIPAA?

A. They will face immediate penalties

B. They will be required to undergo additional training

C. They may avoid severe penalties

D. They will be put on probation

If a covered entity is found to have acted with reasonable cause in failing to comply with HIPAA, they may avoid severe penalties. The concept of "reasonable cause" refers to situations where the entity had a legitimate reason for their actions, even if those actions ultimately resulted in non-compliance. When an investigation determines that a failure to comply was in good faith and not due to willful neglect, the Office for Civil Rights (OCR) has the discretion to impose less severe penalties or even potentially waive penalties altogether. This approach is consistent with HIPAA's goal of promoting compliance and encouraging entities to improve their practices rather than solely focusing on punitive measures. In contrast, if the failure is considered to be the result of willful neglect, the penalties imposed may be much harsher and less forgiving. Thus, recognizing the "reasonable cause" finding allows for some leniency in enforcement actions, which is beneficial for covered entities striving to uphold compliance.

10. Which two identifiers are part of both a limited data set and deidentified information?

A. Telephone number and email address

B. Geographic subdivision and elements of date

C. Full address and birthdate

D. Social security number and medical record number

The correct pairing of identifiers that are part of both a limited data set and deidentified information is geographic subdivision and elements of date. In the context of healthcare privacy, a limited data set is a subset of protected health information (PHI) that excludes certain direct identifiers of the individual or of relatives, employers, or household members of the individual. However, it can include city, state, zip code, and elements of dates (like admissions and discharge dates), which are considered less specific than a full address or birthdate. Deidentified information, on the other hand, refers to data from which personal identifiers have been removed so that individuals cannot be readily identified. For deidentified information, specific geographic subdivisions such as city or town and specific dates are also permissible as they are not direct identifiers. This distinguishes geographic subdivisions and elements of date as identifiers that can be maintained in both contexts, as they provide useful data without exposing an individual's identity directly. Other options like telephone numbers, email addresses, full addresses, birthdates, social security numbers, and medical record numbers are considered direct identifiers and are not included in limited data sets or deidentified data.

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