CERTIFIED IN HEALTHCARE PRIVACY COMPLIANCE (CHPC) PRACTICE EXAM (SAMPLE)

STUDY GUIDE

Prepare with structure. Pass with confidence

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. What action must an entity take in the event of a cyber-attack?

A. Must execute response and mitigation procedures

B. Should report the crime to law enforcement

C. Should report cyber threat indicators to federal agencies

D. All of the above

2. What is the MOST appropriate action for a privacy professional when medical records cannot be located and there is no tracking process?

A. Create shadow records

B. Develop an audit process

C. Design a monitoring tool

D. Recommend discipline

3. Which criteria must be met for a research HIPAA waiver to be approved?

A. The research must not involve any risk

B. The research must pose minimum risk to the patient

C. The research must ensure maximum disclosure

D. The research must involve financial transactions

4. In evaluating the risk of PHI breaches, which employee action is crucial?

A. Preventing all employee interactions with data

B. Monitoring the sharing of passwords

C. Allowing unrestricted access to data

D. Conducting random audits of data access

5. Which act mandates the protection of individual privacy rights related to Federal records?

A. The Freedom of Information Act

B. The Health Insurance Portability and Accountability Act

C. The Privacy Act of 1974

D. The Federal Records Act

SAMPLE

6. Under the HIPAA Security Rule, what type of information is primarily protected?

A. All types of health information

B. Protected Health Information in paper form

C. Protected Health Information in electronic form

D. Health information shared verbally

7. What is a primary objective of the HIPAA Security Rule?

A. To ensure patient satisfaction

B. To promote interoperability of health information systems

C. To protect the confidentiality, integrity, and availability of ePHI

D. To regulate insurance billing practices

8. What is an example of a physical safeguard?

A. Performance reviews

B. Network encryption

C. Locked doors

D. Role-based access

9. What signifies that a violation of PHI is considered a breach?

A. The affected individual's identity is stolen

B. It occurs without authorization

C. The covered entity or Business Associate concludes that the facts constitute a breach

D. The incident is widely known in the media

10. Which federal law is similar to HIPAA in terms of being preempted by more restrictive regulations?

A. 42 CFR Part 3

B. 42 CFR Part 1

C. 42 CFR Part 4

D. 42 CFR Part 2

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What action must an entity take in the event of a cyber-attack?

A. Must execute response and mitigation procedures

B. Should report the crime to law enforcement

C. Should report cyber threat indicators to federal agencies

D. All of the above

In the event of a cyber-attack, an entity should indeed take multiple comprehensive actions to ensure an effective response. Executing response and mitigation procedures is critical; it enables the organization to contain the attack, reduce damage, and initiate recovery processes. This step involves having a well-defined incident response plan that outlines specific actions to be taken immediately following a breach. Reporting the crime to law enforcement is also essential. This not only facilitates a potential investigation into the breach but can also help in preventing future attacks. Law enforcement agencies often have resources and expertise that can aid in dealing with cybercrime. Furthermore, reporting cyber threat indicators to federal agencies contributes to a broader defense strategy against cyber threats. By sharing information about potential vulnerabilities and attack patterns, organizations can help other entities protect themselves and enhance collective cybersecurity efforts. Taking all these actions highlights the multi-faceted approach necessary in responding to a cyber-attack, making the choice to take all these steps the most comprehensive and responsible option.

2. What is the MOST appropriate action for a privacy professional when medical records cannot be located and there is no tracking process?

A. Create shadow records

B. Develop an audit process

C. Design a monitoring tool

D. Recommend discipline

When medical records cannot be located and there is no established tracking process, developing an audit process is the most appropriate action. An audit process serves as a systematic approach to evaluate and improve current practices regarding record management and security. By conducting audits, a privacy professional can identify gaps in practices, examine how and why records are missing, and implement strategies to prevent future occurrences. In the context of healthcare privacy, the integrity and availability of medical records are critical. An audit will help in establishing benchmarks to ensure compliance with regulations such as HIPAA, while also providing insights into any procedural weaknesses. This systematic review can reveal trends or specific areas that require additional training or resources. Creating shadow records, while a potential quick fix, can lead to compliance issues if not handled properly and may create discrepancies within a patient's official medical records. Designing a monitoring tool could be beneficial for ongoing oversight, but it does not address the immediate concerns of missing records. Recommending discipline may be necessary if an individual is found responsible for the oversight, but it doesn't directly resolve the issue of tracking and locating records. Therefore, focusing on an audit process is essential to creating a sustainable solution that enhances the overall management of medical records and compliance with privacy standards.

SAMPLE

3. Which criteria must be met for a research HIPAA waiver to be approved?

A. The research must not involve any risk

B. The research must pose minimum risk to the patient

C. The research must ensure maximum disclosure

D. The research must involve financial transactions

For a research HIPAA waiver to be approved, it is essential that the research poses minimum risk to the patient. This criterion helps protect the privacy and welfare of the individuals involved in the research. The goal of HIPAA regulations is to safeguard patient information while allowing for necessary research activities. Therefore, ensuring that the research has minimal risk to participants is a fundamental requirement. This includes considerations such as how the data will be collected, the potential for harm to the subjects, and the methods used to protect their privacy. It reflects a core principle of ethical research practices, which is to prioritize the safety and rights of participants. Hence, by requiring that the research presents minimal risk, it effectively aligns with the overall objectives of maintaining patient confidentiality and promoting ethical standards within research contexts.

4. In evaluating the risk of PHI breaches, which employee action is crucial?

A. Preventing all employee interactions with data

B. Monitoring the sharing of passwords

C. Allowing unrestricted access to data

D. Conducting random audits of data access

Conducting random audits of data access is crucial in evaluating the risk of PHI (Protected Health Information) breaches because it allows an organization to actively assess how employees interact with sensitive information. These audits provide a mechanism for identifying any unauthorized access, potential misuse of data, or policy violations. By monitoring who accesses PHI, when, and for what purpose, organizations can detect suspicious behaviors, ensure compliance with privacy policies, and implement corrective actions as needed. Random audits help maintain a culture of accountability and support the enforcement of necessary security measures. They are an essential part of a robust risk management strategy and contribute significantly to safeguarding patient information against breaches. Regular audits also enable healthcare organizations to reinforce training and awareness programs to reduce the likelihood of human error, which is often a primary cause of data breaches. In contrast, approaches such as preventing all employee interactions with data are impractical and would likely hinder workflow and operations, while unrestricted access to data poses an inherent risk to patient confidentiality. Similarly, while monitoring the sharing of passwords is important for security, it does not comprehensively assess all the ways that PHI might be mishandled or accessed inappropriately.

SAMPLE

5. Which act mandates the protection of individual privacy rights related to Federal records?

A. The Freedom of Information Act

B. The Health Insurance Portability and Accountability Act

C. The Privacy Act of 1974

D. The Federal Records Act

The Privacy Act of 1974 is the correct answer because it specifically establishes a framework for protecting the privacy of individuals with respect to records maintained by federal agencies. This act governs how personal information is collected, used, and disseminated by federal agencies, allowing individuals to access and amend their records and requiring agencies to maintain accurate and relevant information. It sets forth the requirements for federal agencies to ensure that personally identifiable information is handled with care, limiting disclosure to third parties and establishing safeguards against unauthorized access. The act emphasizes the importance of individual rights in the context of federal record-keeping, thereby directly addressing privacy concerns. In contrast, while the Freedom of Information Act focuses on the public's right to access government information, it does not mandate the protection of individual privacy rights. The Health Insurance Portability and Accountability Act primarily addresses the privacy and security of health information, particularly in the healthcare sector, but is not specific to federal records in general. The Federal Records Act governs the management of federal records, but it does not specifically pertain to individual privacy rights.

6. Under the HIPAA Security Rule, what type of information is primarily protected?

A. All types of health information

B. Protected Health Information in paper form

C. Protected Health Information in electronic form

D. Health information shared verbally

The correct answer focuses on the protection of Protected Health Information (PHI) in electronic form, which is a key aspect of the HIPAA Security Rule. The Security Rule specifically establishes standards for safeguarding electronic PHI (ePHI), which is any health information that is created, received, maintained, or transmitted in electronic format. This includes a wide range of data such as patient records, health insurance information, and treatment records stored electronically. The rationale behind prioritizing ePHI under the Security Rule lies in the increasing use of digital technologies within healthcare, making it critical to protect this sensitive information from potential breaches or unauthorized access. The Security Rule outlines administrative, physical, and technical safeguards that covered entities and business associates must implement to ensure the confidentiality, integrity, and availability of ePHI. Other types of health information, while still important under different aspects of HIPAA, do not fall under the specific provisions of the Security Rule to the same extent as ePHI. For instance, while paper records and verbal communications contain sensitive health information, they are governed more by the Privacy Rule rather than the specific security measures mandated for electronic formats. This focus on ePHI is essential as healthcare continues to evolve in a digitized landscape, emphasizing the need

SAMPLE

7. What is a primary objective of the HIPAA Security Rule?

A. To ensure patient satisfaction

B. To promote interoperability of health information systems

C. To protect the confidentiality, integrity, and availability of ePHI

D. To regulate insurance billing practices

The primary objective of the HIPAA Security Rule is to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). This rule establishes national standards for safeguarding ePHI, which is vital given the increasing reliance on electronic records in healthcare. By focusing on these three key elements—confidentiality ensures that only authorized individuals can access ePHI; integrity guarantees that the information is accurate and unaltered; and availability ensures that the information can be accessed when needed—healthcare organizations can create a secure environment that upholds patient privacy and trust. While ensuring patient satisfaction and promoting interoperability of health information systems are important aspects of healthcare, they are not the primary focus of the HIPAA Security Rule. Similarly, regulating insurance billing practices falls under other provisions of HIPAA but does not relate to the specific goals of security concerning ePHI. Therefore, protecting ePHI is the core intent of the Security Rule, reflecting the importance of safeguarding sensitive health information in a digital landscape.

8. What is an example of a physical safeguard?

A. Performance reviews

B. Network encryption

C. Locked doors

D. Role-based access

A physical safeguard refers to measures that protect the physical environment where health information is stored, processed, or transmitted. Locked doors are a prime example of such a safeguard because they physically restrict access to sensitive areas, such as offices containing personal health information or servers that hold healthcare data. By ensuring that only authorized personnel can enter these spaces, locked doors help prevent unauthorized access and safeguard against theft, loss, or tampering with confidential information. Other options might involve administrative or technical safeguards. For instance, performance reviews relate more to personnel management rather than physical security. Network encryption is a technical safeguard that protects data during transmission, and role-based access is an administrative safeguard that establishes who can access what information based on their job role. While all of these play important roles in overall data security, they do not fall under the definition of physical safeguards.

SAMPLE

9. What signifies that a violation of PHI is considered a breach?

A. The affected individual's identity is stolen

B. It occurs without authorization

C. The covered entity or Business Associate concludes that the facts constitute a breach

D. The incident is widely known in the media

A violation of Protected Health Information (PHI) is classified as a breach when it is assessed based on specific criteria established by privacy regulations, particularly those outlined in the Health Insurance Portability and Accountability Act (HIPAA). When the covered entity or Business Associate analyzes the incident and determines that the facts surrounding it meet the definition of a breach, this indicates that PHI has been accessed, disclosed, or compromised without authorization in a way that poses a risk of harm to individuals. This evaluation process is critical because not all unauthorized access or disclosures are automatically considered breaches. A breach implies a significant risk to the confidentiality and security of the PHI, which can involve factors such as the nature of the information, the unauthorized person who accessed the information, and whether the information was subsequently viewed or acquired. While the other choices mention important scenarios regarding privacy violations, they do not encompass the legal and procedural assessment required to officially deem an incident a breach. For example, the theft of an individual's identity or widespread media coverage might highlight a serious situation but do not serve as definitive indicators of a breach under HIPAA guidelines. The focus is on the unauthorized nature of the event and the consequent evaluation by the applicable parties to confirm that a breach has occurred.

10. Which federal law is similar to HIPAA in terms of being preempted by more restrictive regulations?

A. 42 CFR Part 3

B. 42 CFR Part 1

C. 42 CFR Part 4

D. 42 CFR Part 2

The correct choice is indeed 42 CFR Part 2, which governs the confidentiality of substance use disorder patient records. This regulation is particularly significant because it provides additional protections for alcohol and drug treatment records that go beyond the requirements of HIPAA. Just like HIPAA, which establishes national standards for the protection of health information, 42 CFR Part 2 can be preempted by more restrictive state laws, meaning that if a state law provides a higher level of confidentiality or protection for these records, that state law will take precedence over Part 2. By ensuring that these outcomes are applicable to sensitive categories of health information, 42 CFR Part 2 functions to safeguard individuals seeking treatment for substance use disorders. This similarity in preemption reflects the broader trend of federal regulations allowing for more protective local laws to ensure enhanced privacy and security for vulnerable populations. The other options, while parts of the federal regulations, do not share the same focus on confidential patient records within substance use treatment and thus do not mirror the preemption stance of HIPAA in the same way.

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://healthcareprivacycompliance.examzify.com

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

SAMPLE