HIPAA CLA-100 CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://hipaacla100.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. **Do patients have the right to complain to the federal government if they believe their PHI has been compromised?**

   A. Yes, they can file complaints

   B. No, only if they can prove it

   C. Yes, but only against hospitals

   D. No, they must resolve it internally

2. **What does the term 'Minimum Necessary' mean in relation to PHI?**

   A. Use the least amount of information needed

   B. Share information only with family

   C. Keep all patient information confidential

   D. Determine information based on the situation

3. **What does the "right of access" under HIPAA grant individuals?**

   A. Access to any medical records they desire

   B. Access to their own health information

   C. Access to health information only in emergency situations

   D. Access to information collected by third parties

4. **What does the "90/10" Rule signify in HIPAA compliance?**

   A. 10% of violations come from paperwork errors

   B. 10% of security safeguards are technical and 90% depend on the user

   C. 90% of PHI must be electronic

   D. 10% of healthcare providers handle the majority of data

5. **What does the term 'ePHI' stand for in HIPAA?**

   A. Electronic Personal Health Information

   B. Enhanced Patient Health Information

   C. Emergency Physical Health Information

   D. Expedited Patient Health Information

6. **Which of the following is NOT a goal of HIPAA?**

   A. To ensure health insurance portability

   B. To enhance the privacy of health information

   C. To provide faster payments to healthcare providers

   D. To establish national standards for electronic healthcare transactions

SAMPLE

7. Under HIPAA, which of the following is considered Protected Health Information (PHI)?

A. General statistics about healthcare outcomes

B. Health information that can identify a patient

C. Public health notices

D. Marketing data for health services

8. What does HIPAA stand for?

A. Health Insurance Portability and Accountability Act

B. Health Information Privacy and Accountability Act

C. Health Insurance Privacy and Accessibility Act

D. Health Information Protection and Accountability Act

9. Who must comply with HIPAA regulations?

A. Only healthcare providers

B. Only health insurance companies

C. Covered entities and their business associates

D. Only government-funded healthcare systems

10. What significant updates did the HITECH Act bring to HIPAA?

A. Increased fines for violations

B. Breach notification requirements

C. Both increased fines and breach notifications

D. No changes were made

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Do patients have the right to complain to the federal government if they believe their PHI has been compromised?

A. Yes, they can file complaints

B. No, only if they can prove it

C. Yes, but only against hospitals

D. No, they must resolve it internally

Patients have the right to file complaints with the federal government if they believe their protected health information (PHI) has been compromised. This is an important component of the HIPAA regulations, as it empowers individuals to take action if they feel their privacy rights have been violated. The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) is responsible for enforcing HIPAA privacy protections and accepting complaints related to potential violations. This provision ensures that patients have an official avenue for reporting concerns, which in turn helps to hold covered entities accountable for their handling of PHI. Accessibility of this complaint process reinforces the importance of patient rights within the healthcare system and supports the overall goal of maintaining privacy and security of sensitive health information.

2. What does the term 'Minimum Necessary' mean in relation to PHI?

A. Use the least amount of information needed

B. Share information only with family

C. Keep all patient information confidential

D. Determine information based on the situation

The term 'Minimum Necessary' refers to a foundational principle of the Health Insurance Portability and Accountability Act (HIPAA) concerning the handling of Protected Health Information (PHI). This principle emphasizes that when individuals or organizations access or disclose PHI, they must do so using only the least amount of information necessary to achieve the intended purpose. This ensures that unnecessary exposure of sensitive health information is minimized, thus supporting patient privacy and confidentiality. Utilizing only the minimum necessary information helps healthcare providers, insurers, and business associates limit potential risks associated with unauthorized access or breaches of PHI. It also aligns with HIPAA's overarching goal of protecting personal health information while allowing for essential information sharing for treatment, payment, and healthcare operations. This practice is crucial in balancing patient privacy with the need for information in healthcare. The other options do not reflect the specific intent of the 'Minimum Necessary' standard. Sharing information only with family does not encompass the broader requirement for what is needed in various contexts, while keeping all patient information confidential, while important, does not specifically address the access and sharing of that information. Lastly, determining information based on the situation may incorporate elements of the 'Minimum Necessary' standard but lacks the explicit focus on limiting information to the least amount necessary for

SAMPLE

3. What does the "right of access" under HIPAA grant individuals?

A. Access to any medical records they desire

B. Access to their own health information

C. Access to health information only in emergency situations

D. Access to information collected by third parties

The "right of access" under HIPAA specifically grants individuals the ability to access their own health information. This right empowers patients with the means to obtain and review their medical records, as well as other relevant health information maintained by healthcare providers or health plans. By allowing access to personal health data, HIPAA promotes patient engagement and autonomy in healthcare decision-making. This right includes a broad range of health information, such as records of treatment, test results, and billing information. It is designed to ensure that individuals can verify the accuracy of their medical records, understand their health conditions, and make informed decisions regarding their healthcare. Access is not unlimited or without conditions; there may be specific exceptions or circumstances where access might be restricted, such as in the case of certain psychotherapy notes or when access could harm the individual. However, the premise of the right of access is fundamentally about allowing individuals to see and obtain their own health information, not granting indiscriminate access to any medical records, information only in emergencies, or to third-party information.

4. What does the "90/10" Rule signify in HIPAA compliance?

A. 10% of violations come from paperwork errors

B. 10% of security safeguards are technical and 90% depend on the user

C. 90% of PHI must be electronic

D. 10% of healthcare providers handle the majority of data

The "90/10" Rule in the context of HIPAA compliance emphasizes the significant role that user behavior plays in maintaining the security and privacy of protected health information (PHI). Specifically, this rule indicates that 90% of security safeguards are reliant on the actions and decisions of users, while only 10% of the safeguards are technical in nature. Understanding this principle is vital for organizations because it highlights the fact that even the most advanced technological defenses can be compromised if users do not follow proper protocols or are not adequately trained in security practices. This underscores the importance of user education, training, and adherence to policies designed to protect sensitive information. Implementing effective training programs and ensuring that employees understand the importance of their roles in safeguarding patient information can significantly reduce the likelihood of breaches or violations. The other choices may present interesting information, but they do not accurately capture the essence of the "90/10" Rule as it pertains to user responsibility and the balance of technical versus user-dependent safeguards in HIPAA compliance.

SAMPLE

5. What does the term 'ePHI' stand for in HIPAA?

A. Electronic Personal Health Information

B. Enhanced Patient Health Information

C. Emergency Physical Health Information

D. Expedited Patient Health Information

The term 'ePHI' stands for Electronic Protected Health Information. This refers to any medical information that is created, stored, transmitted, or received in electronic form and is subject to protection under HIPAA regulations. Protected Health Information (PHI) includes any information that can be used to identify an individual and relates to their health, healthcare provision, or payment for healthcare services. Understanding ePHI is critical because HIPAA sets strict standards for safeguarding this type of information to prevent unauthorized access and breaches. Health care providers, health plans, and other entities that handle ePHI must implement appropriate safeguards to maintain confidentiality, integrity, and availability of the electronic health information. The other terms mentioned in the choices do not accurately reflect the definition contained within HIPAA. They do not align with the established definitions used within the regulation, making them incorrect in this context.

6. Which of the following is NOT a goal of HIPAA?

A. To ensure health insurance portability

B. To enhance the privacy of health information

C. To provide faster payments to healthcare providers

D. To establish national standards for electronic healthcare transactions

The primary goals of HIPAA (Health Insurance Portability and Accountability Act) focus on ensuring the privacy and security of health information, maintaining the portability of health insurance, and setting national standards for electronic healthcare transactions. Among the provided options, the goal of providing faster payments to healthcare providers is not explicitly mentioned as one of HIPAA's objectives. HIPAA was created to protect individuals' medical records and other personal health information and to ensure that individuals can maintain health insurance coverage when changing or losing jobs. It also aims to standardize electronic data exchange in healthcare, ensuring that healthcare providers adhere to uniform standards for processing health records and transactions. While improvements in payment processes may be a side benefit of the standardization that HIPAA facilitates, faster payments themselves are not a defined goal of the legislation. Thus, the statement that suggests faster payments is not aligned with the primary objectives of HIPAA makes it the correct choice.

SAMPLE

7. Under HIPAA, which of the following is considered Protected Health Information (PHI)?

A. General statistics about healthcare outcomes

B. Health information that can identify a patient

C. Public health notices

D. Marketing data for health services

Protected Health Information (PHI) under HIPAA is defined as any health information that is created, received, or maintained by a covered entity that can be used to identify an individual. This includes information related to the individual's past, present, or future physical or mental health condition, the provision of healthcare to the individual, or the payment for the provision of healthcare. The correct answer focuses on the aspect of health information that carries the potential to identify a specific patient. This identification may include names, addresses, birthdates, Social Security numbers, and any other information that can trace back to an individual. Given that this information is sensitive, HIPAA establishes strict regulations to protect it, ensuring that individuals' privacy is preserved. The other options do not meet the criteria for PHI as defined by HIPAA. General statistics about healthcare outcomes are aggregated data that do not identify individuals and therefore do not qualify as PHI. Public health notices are often related to health trends or communicable diseases and do not include personal identifiers. Marketing data for health services typically involves non-specific information about services or populations and does not pertain directly to an individual patient's health information. Thus, only health information capable of identifying a patient is classified as PHI under HIPAA.

8. What does HIPAA stand for?

A. Health Insurance Portability and Accountability Act

B. Health Information Privacy and Accountability Act

C. Health Insurance Privacy and Accessibility Act

D. Health Information Protection and Accountability Act

HIPAA stands for the Health Insurance Portability and Accountability Act. This legislation, enacted in 1996, primarily aims to enhance the efficiency and effectiveness of the healthcare system by establishing standards for the electronic exchange of health information. It also focuses on protecting the privacy and security of individuals' medical records and other personal health information. The correct choice accurately reflects the full title of the act, which emphasizes both the portability of health insurance for individuals—meaning that employees can maintain their health coverage when they change jobs—and the accountability aspects related to safeguarding sensitive health information. Understanding the precise definition and intent of HIPAA is crucial for navigating compliance in healthcare settings and protecting patient rights.

SAMPLE

9. Who must comply with HIPAA regulations?

A. Only healthcare providers

B. Only health insurance companies

C. Covered entities and their business associates

D. Only government-funded healthcare systems

The correct response highlights that compliance with HIPAA regulations is a requirement for covered entities and their business associates. Covered entities include healthcare providers who transmit health information electronically, health insurance companies, and healthcare clearinghouses. These entities are directly responsible for safeguarding protected health information (PHI) and ensuring its confidentiality, integrity, and availability. Business associates are individuals or entities that perform functions or services on behalf of covered entities that involve the use or disclosure of PHI. They are also held accountable under HIPAA, as they must adhere to specific privacy and security requirements when handling health information. This dual layer of accountability ensures that not just healthcare providers and insurers, but also those who work with them, are committed to protecting sensitive health data. The other options suggest a narrower interpretation of who must comply with HIPAA, focusing on only specific types of entities, which does not capture the full spectrum of responsibilities defined by the regulations.

10. What significant updates did the HITECH Act bring to HIPAA?

A. Increased fines for violations

B. Breach notification requirements

C. Both increased fines and breach notifications

D. No changes were made

The HITECH Act made significant amendments to HIPAA, primarily aimed at enhancing the protection of sensitive health information. One of the key updates brought by this legislation was the introduction of increased fines for violations of HIPAA regulations. This change was intended to strengthen enforcement and encourage compliance by imposing higher penalties on organizations that failed to safeguard protected health information (PHI). Additionally, the HITECH Act established breach notification requirements, which mandated that covered entities and their business associates notify individuals in the event of a breach of unsecured PHI. This requirement enhanced transparency and empowered patients to take immediate action if their information was compromised. By combining both increased fines for violations and the implementation of breach notification requirements, the HITECH Act significantly bolstered HIPAA's framework for protecting patient information and promoting accountability among healthcare providers and related entities. This dual impact underscores why the correct answer encapsulates both of these critical updates.

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://hipaacla100.examzify.com

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

SAMPLE