HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPPA) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://hippa.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. Where can one find the latest changes to HIPAA law?

A. The White House Website

B. Department of Health and Human Services (DHHS) Website

C. Centers for Medicare and Medicaid Services (CMS) Website

D. Health and Human Services Agency Website

2. What categories of entities did the law passed by Congress in 1996 mandate identifiers for?

A. Healthcare providers, health plans, patients, employers

B. Insurance agents, patients, hospitals, employers

C. Government agencies, health providers, pharmacies, patients

D. Employers, health insurance brokers, health plans, caregivers

3. Which of the following situations does NOT require a Business Associate Contract?

A. When PHI is shared

B. With organizations that act solely as a conduit for PHI

C. When healthcare services are provided

D. When financial transactions occur

4. Who must a Business Associate report a breach of protected health information (PHI) to?

A. The patient's family

B. The covered entity responsible for the original health information

C. The federal government

D. Insurance companies

5. What does the security of e-PHI relate to?

A. Access control procedures

B. Data breach prevention

C. Storing patient records

D. All of the above

SAMPLE

6. What is the primary purpose of technical safeguards?

A. Protecting physical access to files

B. Managing workforce behavior regarding PHI

C. Protecting and controlling access to ePHI

D. Creating health policies

7. Which entities must comply with HIPAA regulations?

A. Covered Entities and Beneficiaries.

B. Covered Entities and Business Associates.

C. Business Associates and Third Parties.

D. Covered Entities and Employers.

8. Authorization is not required to disclose protected health information (PHI) in which of the following scenarios?

A. Research studies

B. Patient treatment and payment purposes

C. Marketing purposes

D. Employment-related disclosures

9. Which of the following statements is TRUE regarding the HITECH and Omnibus updates?

A. It guarantees portability of health insurance coverage

B. It requires breach notifications under specific circumstances

C. It relaxes rules on PHI access by business associates

D. It limits patient rights to amend their health records

10. What type of information is NOT typically classified as PHI?

A. A patient's name and medical records

B. Health information that cannot identify an individual

C. A diagnosis and treatment records

D. A patient's social security number

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Where can one find the latest changes to HIPAA law?

A. The White House Website

B. Department of Health and Human Services (DHHS) Website

C. Centers for Medicare and Medicaid Services (CMS) Website

D. Health and Human Services Agency Website

The Department of Health and Human Services (DHHS) website is the most authoritative source for the latest changes to HIPAA law. The DHHS oversees the administration of HIPAA and provides updates, guidance, and resources relevant to the law's implementation and enforcement. This includes changes, clarifications, and additions to regulations that are necessary to adapt to evolving healthcare practices and technologies. While the other websites mentioned may provide relevant healthcare information, they do not specifically centralize updates regarding HIPAA law. The White House website typically focuses on broader policy initiatives, while the Centers for Medicare and Medicaid Services (CMS) deals primarily with Medicare and Medicaid programs, and the Health and Human Services Agency may refer to state-level departments that do not have the same central role in HIPAA regulation as the DHHS. Therefore, the DHHS website is indeed the most reliable and direct source for the most current HIPAA information.

2. What categories of entities did the law passed by Congress in 1996 mandate identifiers for?

A. Healthcare providers, health plans, patients, employers

B. Insurance agents, patients, hospitals, employers

C. Government agencies, health providers, pharmacies, patients

D. Employers, health insurance brokers, health plans, caregivers

The law passed by Congress in 1996, known as the Health Insurance Portability and Accountability Act (HIPAA), established a framework for the protection of health information and designated specific entities that would be subject to identifiers. The correct answer encompasses healthcare providers, health plans, and employers as the primary entities for which identifiers were mandated. Healthcare providers are essential in ensuring the delivery of medical services and managing patient information, and they require unique identifiers to streamline transactions and maintain confidentiality. Health plans, which include various forms of insurance, also need identifiers to facilitate the handling of claims and coverage details. Additionally, employers play a critical role, as they typically provide health insurance to their employees and must navigate the administrative aspects of health benefits. This combination signifies the law's attention to key participants in the healthcare system, ensuring that there is a standardized method for identification that enhances the accountability and efficiency of healthcare operations while also safeguarding patient privacy.

SAMPLE

3. Which of the following situations does NOT require a Business Associate Contract?

A. When PHI is shared

B. With organizations that act solely as a conduit for PHI

C. When healthcare services are provided

D. When financial transactions occur

A Business Associate Contract (BAC) is necessary whenever a third party handles Protected Health Information (PHI) on behalf of a covered entity, except in certain situations. In the case where organizations act solely as conduits for PHI, they do not have access to the PHI beyond what is necessary for the transmission, and they are not involved in the management or use of that information. This means that they are not considered business associates and, therefore, do not require a Business Associate Contract. For the other situations mentioned, a BAC is essential because these entities may manage or have access to PHI in ways that could impact the privacy and security of the information. In healthcare services provision, for example, the service providers are actively involved in handling PHI, necessitating a formal agreement to ensure compliance with HIPAA regulations.

4. Who must a Business Associate report a breach of protected health information (PHI) to?

A. The patient's family

B. The covered entity responsible for the original health information

C. The federal government

D. Insurance companies

A Business Associate is required under HIPAA regulations to report any breaches of protected health information (PHI) to the covered entity that is responsible for the original health information. This is because the covered entity holds the primary obligation for ensuring the confidentiality, integrity, and availability of PHI. When a breach occurs, the Business Associate must inform the covered entity promptly so that it can take the necessary steps to mitigate any harm, notify affected individuals if required, and comply with federal and state regulations regarding breach notification. This responsibility emphasizes the importance of communication between the Business Associate and the covered entity, ensuring that patient information is adequately protected and that appropriate actions can be taken in response to any incidents. The other options involve parties that are not typically involved in the formal breach notification process established under HIPAA regulations. For example, notifying a patient's family or insurance companies does not fulfill the legal obligation regarding breaches; thus, these parties are not the correct recipients of such reports. The requirement for notifying the federal government is also separate and typically only applies under specific circumstances and not for every breach reported by a Business Associate.

SAMPLE

5. What does the security of e-PHI relate to?

A. Access control procedures

B. Data breach prevention

C. Storing patient records

D. All of the above

The security of electronic Protected Health Information (e-PHI) encompasses various aspects designed to protect sensitive health data, ensuring its confidentiality, integrity, and availability. When we discuss access control procedures, they are fundamental to security as they regulate who can access e-PHI and under what circumstances, preventing unauthorized access. Data breach prevention directly addresses the risk of exposure to e-PHI, implementing measures to guard against unauthorized disclosures or breaches. Storing patient records involves ensuring that e-PHI is securely stored, often through encryption and proper database management, to protect against data loss or theft. Since security means addressing multiple interconnected areas, the correct understanding is that encompassing all these elements—access control, breach prevention, and secure storage—is essential for comprehensive protection of e-PHI. Hence, a holistic approach is necessary, which is what the all-encompassing option signifies; it captures the multi-faceted nature of e-PHI security.

6. What is the primary purpose of technical safeguards?

A. Protecting physical access to files

B. Managing workforce behavior regarding PHI

C. Protecting and controlling access to ePHI

D. Creating health policies

The primary purpose of technical safeguards is to protect and control access to electronic protected health information (ePHI). Technical safeguards are critical components outlined in the Health Insurance Portability and Accountability Act (HIPAA) that establish the technological measures used to secure ePHI from unauthorized access. These safeguards include methods such as encryption, access control, and audit controls that ensure only authorized users can access specific types of health information. By implementing technical safeguards, healthcare entities can minimize risks associated with data breaches and ensure the confidentiality, integrity, and availability of ePHI. It is essential to understand that while protecting physical access and creating policies are important in the overall security framework, they fall under different categories, such as physical safeguards and administrative safeguards, respectively. Therefore, the focus of technical safeguards is solely on the technological aspects of protecting electronic health information.

SAMPLE

7. Which entities must comply with HIPAA regulations?

A. Covered Entities and Beneficiaries.

B. Covered Entities and Business Associates.

C. Business Associates and Third Parties.

D. Covered Entities and Employers.

The correct answer identifies that both Covered Entities and Business Associates must comply with HIPAA regulations. Covered Entities include healthcare providers who transmit any health information in electronic form in connection with a HIPAA transaction, health plans, and healthcare clearinghouses. These organizations handle protected health information (PHI) and thus have strict obligations to safeguard that information and ensure its confidentiality and integrity. Business Associates are individuals or entities that perform certain functions or activities on behalf of or provide certain services to, a Covered Entity that involve the use or disclosure of PHI. Even though they are not directly responsible for providing healthcare, Business Associates are required to comply with HIPAA rules to protect PHI when they handle data on behalf of Covered Entities. This compliance includes entering into Business Associate Agreements with Covered Entities, which outline the responsibilities of all parties regarding the handling of PHI. Other options include entities which do not fall under the specific compliance mandates set forth in HIPAA. Beneficiaries are individuals receiving health benefits and do not have compliance obligations. Third Parties may not necessarily have access to PHI in a manner that requires compliance, and while employers may possess information relevant to health plans, they do not directly handle PHI as defined by HIPAA unless they are acting in the role

8. Authorization is not required to disclose protected health information (PHI) in which of the following scenarios?

A. Research studies

B. Patient treatment and payment purposes

C. Marketing purposes

D. Employment-related disclosures

The scenario of patient treatment and payment purposes is a situation where authorization is not required to disclose protected health information (PHI). Under the Health Insurance Portability and Accountability Act (HIPAA), covered entities are permitted to share PHI as necessary to provide treatment to a patient and to obtain payment for those services. This provision facilitates efficient health care delivery by allowing healthcare providers to communicate about a patient's care without needing to secure explicit consent for every individual interaction. For instance, a doctor can share relevant information with a specialist for the purpose of coordinating care, or a healthcare provider can send a bill to an insurance company without patient authorization. In contrast, disclosing PHI for research studies, marketing purposes, or employment-related disclosures generally requires specific authorization from the individual, as these uses are not directly related to the treatment or payment involved in healthcare delivery. This distinction helps protect patients' privacy while still enabling essential healthcare operations to proceed efficiently.

SAMPLE

9. Which of the following statements is TRUE regarding the HITECH and Omnibus updates?

A. It guarantees portability of health insurance coverage

B. It requires breach notifications under specific circumstances

C. It relaxes rules on PHI access by business associates

D. It limits patient rights to amend their health records

The statement that requires breach notifications under specific circumstances is accurate concerning the HITECH and Omnibus updates. These updates enhanced the privacy and security protections established by HIPAA and imposed stricter requirements for notifying individuals impacted by a data breach. Specifically, covered entities and business associates are mandated to provide notification when a breach involving unsecured protected health information (PHI) occurs. This regulation aims to ensure that individuals are informed promptly, allowing them to take necessary precautions to protect themselves from potential harm resulting from the breach. In contrast, the other statements do not align with the updates' objectives or stipulations. While the act focuses on portability, it does not guarantee coverage portability itself. The updates do not relax rules on PHI access by business associates; instead, they tighten security measures. Lastly, patient rights to amend their health records remain protected, without imposing limitations under the recent updates. This framework underscores the ongoing commitment to safeguarding personal health information in the evolving digital landscape.

10. What type of information is NOT typically classified as PHI?

A. A patient's name and medical records

B. Health information that cannot identify an individual

C. A diagnosis and treatment records

D. A patient's social security number

Health information that cannot identify an individual is not classified as protected health information (PHI) under HIPAA. PHI encompasses any data that can be used to identify an individual in conjunction with their health information, including personal details such as names, medical records, diagnoses, treatment records, and social security numbers. When information is de-identified, meaning that all identifiers have been removed or a method has been applied to ensure that it cannot be linked back to an individual, it no longer falls under the protections of HIPAA. This distinction is crucial because HIPAA's regulations are designed to safeguard the privacy and security of identifiable health information. Therefore, in situations where health information does not relate to an identifiable individual, it does not qualify as PHI, allowing for its use without the same stringent requirements set forth by HIPAA.

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://hippa.examzify.com

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

SAMPLE