Certified in Healthcare Privacy Compliance (CHPC) Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit:
https://healthcareprivacycompliance.examzify.com

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

Table of Contents

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.

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!

Questions

1. A breach is assumed unless the covered entity can demonstrate what?

- **A. High probability of data compromise**
- **B. Low probability of data compromise**
- **C. No harm to any individual involved**
- **D. Complete recovery of PHI data**

2. What is considered a "Covered Entity" under HIPAA?

- **A. An organization that provides health services**
- **B. A health insurance organization**
- **C. A personal data aggregator company**
- **D. A provider, health plan, or clearinghouse that transmits health information electronically**

3. Which method is NOT recognized for de-identifying PHI?

- **A. Expert Determination (Statistical) de-identification**
- **B. Safe harbor method**
- **C. Aggregation**
- **D. None of the above**

4. What type of records must be created for children with special health care needs according to ADA requirements?

- **A. Nursing records**
- **B. Individual health plans**
- **C. Health assessment records**
- **D. Education records**

5. Which of the following is a valid example of using or disclosing PHI outside of treatment, payment, or healthcare operations?

- **A. Professional networking**
- **B. Organ/tissue donation decedent information**
- **C. Marketing services to individuals**
- **D. Nonprofit fundraising**

6. **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

7. **What is the primary focus of a Security Risk Analysis?**

   A. To assess employee performance in data management

   B. To identify security measures that need to be implemented

   C. To evaluate patient satisfaction regarding privacy

   D. To determine the financial impact of security violations

8. **What does unsecured PHI refer to according to HHS Secretary's guidance?**

   A. PHI that is under complete lock and key

   B. PHI that is incompletely documented

   C. PHI that cannot be deciphered by unauthorized persons

   D. PHI that is not rendered unusable, unreadable, or indecipherable by specific technology or methodology

9. **How does a patient learn about privacy under HIPAA?**

   A. He looks it up on the internet.

   B. The government sent this out in the mail to every U.S. Citizen prior to April 14, 2003.

   C. He asks his doctor or nurse.

   D. At the patient's first visit, he is given the Provider's Notice of Privacy Practices and signs an acknowledgment.

10. **Which of the following statements about PHI is correct?**

   A. PHI only includes physical conditions.

   B. PHI applies to all health care providers.

   C. PHI can contain identifiers related to patients.

   D. PHI is never shared without consent.

Answers

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

Explanations

1. A breach is assumed unless the covered entity can demonstrate what?

- A. High probability of data compromise
- B. Low probability of data compromise
- C. No harm to any individual involved
- D. Complete recovery of PHI data

A breach of protected health information (PHI) is generally presumed unless the covered entity can demonstrate a low probability that the information has been compromised. This means that the covered entity must provide evidence or assurance that despite the incident, the likelihood of any PHI being improperly accessed or disclosed is minimal. When a breach occurs, the covered entity has the burden of proof to show that the breach did not compromise the integrity or confidentiality of the information. This is often assessed through a risk assessment, which evaluates factors such as the nature of the data, the unauthorized person’s access to the data, whether the data was actually acquired or viewed, and the extent to which the risk to patient data has been mitigated. In contrast, if a high probability of data compromise is demonstrated, it confirms the breach, while harm or complete recovery of the data does not negate the possibility of a breach. Thus, the focus on demonstrating a low probability of compromise aligns with regulatory standards aimed at protecting patient privacy and maintaining the security of sensitive information.

2. What is considered a "Covered Entity" under HIPAA?

- A. An organization that provides health services
- B. A health insurance organization
- C. A personal data aggregator company
- D. A provider, health plan, or clearinghouse that transmits health information electronically

A "Covered Entity" under HIPAA includes providers, health plans, and healthcare clearinghouses that transmit health information in electronic form. This definition is crucial in understanding the scope of HIPAA regulations, which are designed to protect the privacy and security of individuals' health information. Covered Entities play a significant role in the healthcare system as they are directly involved in the handling of protected health information (PHI). For instance, healthcare providers such as doctors and hospitals that bill electronically for services fall under this category. Health plans, which include insurance companies that pay for healthcare services, and clearinghouses that process or facilitate the transmission of health information, are also included. The focus on electronic transmission is particularly important because HIPAA was established to address the increasing use of electronic records and communications in the healthcare sector, thereby necessitating regulations to safeguard sensitive patient information. Understanding this definition helps clarify how HIPAA applies to various organizations involved in healthcare, emphasizing the protective measures these entities must adhere to regarding patient privacy.

3. Which method is NOT recognized for de-identifying PHI?

A. Expert Determination (Statistical) de-identification

B. Safe harbor method

C. Aggregation

D. None of the above

The method identified in the question as not recognized for de-identifying protected health information (PHI) is aggregation. De-identification is a critical process in healthcare that aims to protect patient privacy by removing identifying information from health data, making it impossible to link the data to a specific individual. The expert determination method relies on statistical or scientific principles to ensure that the risk of re-identification is very small, using qualified experts to assess and confirm this level of risk. This method is widely recognized and employed in various healthcare contexts for de-identifying data. The safe harbor method provides a standard approach, where specific identifiers are removed from the data, including names, geographical identifiers smaller than a state, and other elements that could create a risk of identifying the individual. This method is also officially recognized and commonly used to achieve de-identification. In contrast, aggregation refers to the process of combining data points or information to create a summary or model; while useful for analysis, aggregation does not sufficiently remove individual identifiers or reduce the risk of re-identification in the manner that the other recognized methods do. Hence, it is not considered a valid method for de-identifying PHI according to established standards and regulations in healthcare privacy compliance.

4. What type of records must be created for children with special health care needs according to ADA requirements?

A. Nursing records

B. Individual health plans

C. Health assessment records

D. Education records

The correct answer relates specifically to ADA requirements, which mandate that individuals with disabilities, including children with special health care needs, are entitled to appropriate educational accommodations and supports. Education records are crucial in this context as they document the student’s progress, health-related needs, and services received within the educational setting. These records serve not only to facilitate compliance with the ADA but also to ensure that children receive the necessary support to access their education effectively. In the case of children with special health care needs, education records would encompass individualized education plans (IEPs) and any related health accommodations, making sure that their specific needs are addressed in school. This holistic view ensures that educational institutions abide by legal obligations and provide an inclusive environment. Other options, such as nursing records, individual health plans, and health assessment records, while they may be relevant in a healthcare or clinical context, do not directly align with the focus of the ADA on education and the rights of students with disabilities. They may provide essential information about a child's health but do not focus on their educational needs linked to the ADA requirements.

5. Which of the following is a valid example of using or disclosing PHI outside of treatment, payment, or healthcare operations?

A. Professional networking

B. Organ/tissue donation decedent information

C. Marketing services to individuals

D. Nonprofit fundraising

The selection of organ/tissue donation decedent information as a valid example of using or disclosing protected health information (PHI) outside of treatment, payment, or healthcare operations is accurate due to the specific regulatory requirements surrounding organ and tissue donation. According to the Health Insurance Portability and Accountability Act (HIPAA) and related healthcare regulations, organizations may disclose the necessary PHI for the purposes of organ and tissue donation and transplantation. This disclosure is deemed appropriate because it serves a critical public health objective—facilitating the donation process that can ultimately save lives. When healthcare providers are involved in situations where they need to ascertain organ or tissue viability from decedents, important information regarding PHI is shared with organ procurement organizations. This type of disclosure is accepted under the regulations as it is directly tied to a benevolent purpose that extends beyond standard healthcare operations. In contrast, options like professional networking, marketing services to individuals, and nonprofit fundraising typically require more stringent controls and may not fit within the established exemptions for using or disclosing PHI outside the scope of treatment, payment, or healthcare operations without required patient authorization or specific compliance measures in place.

6. 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.

7. What is the primary focus of a Security Risk Analysis?

A. To assess employee performance in data management

B. To identify security measures that need to be implemented

C. To evaluate patient satisfaction regarding privacy

D. To determine the financial impact of security violations

The primary focus of a Security Risk Analysis is to identify security measures that need to be implemented. This analysis involves a thorough examination of the current security environment within a healthcare organization to determine potential vulnerabilities and threats to sensitive data. Conducting a Security Risk Analysis allows an organization to pinpoint areas where security enhancements are necessary to safeguard protected health information (PHI) and comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Through this process, organizations identify specific risks and the likelihood of their occurrence, enabling them to prioritize their remediation efforts effectively. This proactive approach helps ensure that necessary security controls are established or strengthened to protect against unauthorized access, data breaches, and other threats to patient information. While assessing employee performance in data management, evaluating patient satisfaction regarding privacy, and determining the financial impact of security violations are valuable activities, they do not directly address the fundamental purpose of a Security Risk Analysis, which is specifically geared towards identifying and mitigating security risks related to data handling and protection.

8. What does unsecured PHI refer to according to HHS Secretary's guidance?

A. PHI that is under complete lock and key

B. PHI that is incompletely documented

C. PHI that cannot be deciphered by unauthorized persons

D. PHI that is not rendered unusable, unreadable, or indecipherable by specific technology or methodology

Unsecured PHI refers to protected health information that has not been adequately protected using certain technologies or methodologies, making it accessible and potentially understandable to unauthorized individuals. According to guidance from the HHS Secretary, this definition emphasizes that PHI needs to be rendered unusable, unreadable, or indecipherable to be considered secure. For example, encryption or destruction of the data are methods that ensure the information remains protected. If PHI is not rendered unusable, unreadable, or indecipherable through the application of appropriate safeguards, it is deemed unsecured, which can lead to breaches of patient privacy and potential legal ramifications. This aspect is crucial in healthcare compliance as it emphasizes the importance of taking proactive steps to secure sensitive patient information from unauthorized access.

9. How does a patient learn about privacy under HIPAA?

A. He looks it up on the internet.

B. The government sent this out in the mail to every U.S. Citizen prior to April 14, 2003.

C. He asks his doctor or nurse.

D. At the patient's first visit, he is given the Provider's Notice of Privacy Practices and signs an acknowledgment.

The correct answer highlights a fundamental aspect of patient rights and the communication of privacy practices under HIPAA (Health Insurance Portability and Accountability Act). During a patient's initial visit to a healthcare provider, it is standard practice for the provider to present the Notice of Privacy Practices. This document outlines how the patient's medical information may be used and shared, as well as the individual's rights regarding their health information. By providing this notice at the first visit, healthcare organizations ensure that patients are adequately informed about their privacy rights and the specific practices in place to safeguard their personal health information. This process of direct communication is essential for fostering transparency and trust between patients and their healthcare providers. Moreover, the requirement for patients to sign an acknowledgment further reinforces their understanding of the privacy policies in effect. This proactive approach helps to educate patients about their rights and the importance of privacy in healthcare settings, aligning with HIPAA's objectives to protect patient information and enhance confidentiality. In contrast, while looking up information on the internet can provide some insights into HIPAA, it does not guarantee that the patient receives accurate, tailored information from their specific provider. Similarly, while patients can inquire about privacy practices from their healthcare providers, the formal process of providing the Notice of Privacy Practices is mandated to ensure every

10. Which of the following statements about PHI is correct?

A. PHI only includes physical conditions.

B. PHI applies to all health care providers.

C. PHI can contain identifiers related to patients.

D. PHI is never shared without consent.

The statement that PHI can contain identifiers related to patients is correct because Protected Health Information (PHI) is defined under the Health Insurance Portability and Accountability Act (HIPAA) and encompasses a wide range of information. This includes any data that can identify an individual and relates to their health status, healthcare provision, or payment for healthcare. Identifiers may include names, addresses, dates of birth, Social Security numbers, and any other information that can link the data to an individual. The inclusion of these identifiers is a key aspect of what constitutes PHI, which is designed to protect the individual's privacy and security of their health information. In contrast, the other statements do not fully capture the scope and regulations surrounding PHI. For example, stating that PHI only includes physical conditions is inaccurate because PHI encompasses mental health information, treatment, and payment details, not just physical health data. The assertion that PHI applies to all health care providers is misleading, as it specifically applies to covered entities and business associates that handle such information, not to every individual or organization that may be involved in healthcare. Finally, while consent is typically required before sharing PHI, there are certain circumstances under which PHI can be shared without consent, such as for public

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!