CERTIFIED INFORMATION PRIVACY PROFESSIONAL (CIPP) PRACTICE QUESTIONS (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cipp.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 category of law best describes the HIPAA Privacy Rule?

A. Constitutional law

B. Common law

C. Legislative law

D. Administrative law

2. Which firm was charged with an unfair trade practice for collecting information from mobile devices without consent?

A. DesignerWare

B. Wyndham

C. Snapchat

D. Nomi

3. Which law contains a private right of action?

A. CCPA

B. FERPA

C. GLBA

D. HIPAA

4. What is not a common responsibility of an organization's chief privacy officer?

A. Managing privacy risks

B. Encrypting personal information

C. Developing privacy information

D. Advocating privacy strategies

5. Which one of the following laws includes a data breach notification requirement that applies to many different categories of personal information?

A. GDPR

B. HIPAA

C. GLBA

D. FERPA

SAMPLE

6. What is the smallest population size for which ZIP codes can be retained according to HHS guidelines for de-identifying records?

A. 1,000

B. 2,000

C. 10,000

D. 20,000

7. What is the primary purpose of the Privacy Protection Act (PPA)?

A. Regulate the electronic monitoring of employees.

B. Provide privacy for journalists and protect their work product.

C. Enhance consumer privacy in financial transactions.

D. Govern government access to personal information.

8. What federal privacy law contains specific requirements for how organizations must dispose of sensitive personal information?

A. FERPA

B. FACTA

C. GLBA

D. SOX

9. Which law imposes specific requirements on the disposal of consumer report information?

A. Health Insurance Portability and Accountability Act (HIPAA)

B. Fair and Accurate Credit Transactions Act (FACTA)

C. Gramm-Leach-Bliley Act (GLBA)

D. Sarbanes-Oxley Act (SOX)

10. Which U.S. federal law is most comparable to the EU's GDPR?

A. The Patriot Act

B. The Privacy Act

C. None

D. The Civil Rights Act

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What category of law best describes the HIPAA Privacy Rule?

A. Constitutional law

B. Common law

C. Legislative law

D. Administrative law

The HIPAA Privacy Rule is classified as administrative law because it was established through the regulatory process of an administrative agency, specifically the U.S. Department of Health and Human Services (HHS). Administrative law refers to the body of law that governs the activities of administrative agencies of government. The HIPAA Privacy Rule sets standards for protecting sensitive patient health information, which falls under the jurisdiction of HHS. These regulations are created to enforce and interpret existing legislation—in this case, the Health Insurance Portability and Accountability Act (HIPAA) itself. Administrative law is critical in the healthcare sector, as it governs how agencies create and enforce rules to ensure the protection of individuals' privacy rights. In contrast, constitutional law involves interpreting the Constitution and applying its principles to cases, common law refers to laws developed through court decisions rather than through statutes, and legislative law pertains more directly to laws enacted by legislative bodies, such as Congress. Therefore, while HIPAA stems from legislative intent, its implementation and the specific regulations derived from it are best categorized under administrative law.

2. Which firm was charged with an unfair trade practice for collecting information from mobile devices without consent?

A. DesignerWare

B. Wyndham

C. Snapchat

D. Nomi

Nomi was charged with an unfair trade practice for collecting information from mobile devices without obtaining explicit consent from users. The firm was found to have engaged in practices related to gathering location data from mobile devices in retail environments, which raised significant privacy concerns. Nomi's methods involved tracking the locations and behaviors of customers without proper acknowledgment or permission, leading to scrutiny over whether they were transparently informing users about their data collection practices. This case highlighted broader issues about consumer privacy and the importance of consent in data collection, particularly in mobile contexts where users may not be fully aware of what data is being collected or how it will be used. The legal action reflected growing regulatory attention on privacy practices in the digital landscape and underscored the necessity for companies to prioritize consumer consent in their data collection strategies.

SAMPLE

3. Which law contains a private right of action?

A. CCPA

B. FERPA

C. GLBA

D. HIPAA

The California Consumer Privacy Act (CCPA) includes a private right of action, allowing consumers to sue businesses for certain violations, particularly in cases of data breaches that expose personal information. This provision empowers individuals to take legal action if they believe their privacy rights under the CCPA have been violated, highlighting the act's focus on consumer control over personal data and ensuring accountability among businesses regarding data protection practices. In contrast, the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA) do not provide individuals with a private right of action for enforcement. Instead, these laws establish specific regulatory mechanisms or allow enforcement only by designated agencies or the federal government, limiting individuals' capacity to directly pursue legal claims in cases of non-compliance.

4. What is not a common responsibility of an organization's chief privacy officer?

A. Managing privacy risks

B. Encrypting personal information

C. Developing privacy information

D. Advocating privacy strategies

The role of a Chief Privacy Officer (CPO) primarily focuses on strategic responsibilities related to data privacy management within an organization. While they play a crucial part in the overall privacy framework, their duties typically revolve around managing privacy risks, developing privacy policies and programs, and advocating for effective privacy strategies that comply with legal and regulatory standards. Encrypting personal information, while an essential aspect of data protection, is generally a technical responsibility that falls under the purview of IT departments or information security professionals. The CPO may advocate for encryption measures and ensure that policies mandate encryption, but they are not usually directly involved in the implementation of these technical solutions. This distinction highlights why encrypting personal information is not typically a responsibility that the CPO would undertake, making it the correct answer in this context.

SAMPLE

5. Which one of the following laws includes a data breach notification requirement that applies to many different categories of personal information?

A. GDPR

B. HIPAA

C. GLBA

D. FERPA

The General Data Protection Regulation (GDPR) is a comprehensive data protection law in the European Union that mandates a data breach notification requirement applicable to various types of personal information. Under GDPR, organizations must notify individuals without undue delay when there is a high risk to their rights and freedoms resulting from a personal data breach. This law emphasizes transparency and accountability, requiring not only the notification of affected individuals but also, in certain circumstances, the notification of the relevant supervisory authority. In contrast, while HIPAA does require data breach notifications, it is specific to health information and primarily applies to healthcare providers, health plans, and business associates handling protected health information. The GLBA focuses on protecting consumers' private financial information, and while it includes privacy provisions, it does not have a broad data breach notification requirement for various types of personal data like GDPR. FERPA protects student educational records and has specific requirements related to student privacy but is not as inclusive of different categories of personal information as GDPR. This broad applicability of GDPR to numerous data types makes it the most relevant answer in the context of data breach notification requirements.

6. What is the smallest population size for which ZIP codes can be retained according to HHS guidelines for de-identifying records?

A. 1,000

B. 2,000

C. 10,000

D. 20,000

The Health and Human Services (HHS) guidelines for the de-identification of records specify that when using ZIP codes to retain identifying information, the minimum population size associated with that ZIP code must be 20,000 residents. This guideline is intended to ensure that the de-identified data maintains anonymity and mitigates the risk of re-identification, which can occur in smaller population sets. In essence, if a ZIP code corresponds to a geographic area with fewer than 20,000 individuals, there is a higher likelihood that specific individuals could be identified within that area, thus compromising the privacy of the data subjects. Therefore, the requirement of a 20,000 population threshold serves as a crucial standard to protect the privacy of individuals in datasets while allowing certain geographic information to be used in a controlled manner. This threshold reflects a broader principle in data privacy that seeks to balance the utility of data with the need for confidentiality and protection of personal information.

SAMPLE

7. What is the primary purpose of the Privacy Protection Act (PPA)?

A. Regulate the electronic monitoring of employees.

B. Provide privacy for journalists and protect their work product.

C. Enhance consumer privacy in financial transactions.

D. Govern government access to personal information.

The Privacy Protection Act (PPA) was established to specifically safeguard the work of journalists and their ability to gather and disseminate news without undue interference from law enforcement or government entities. The primary intention behind this legislation is to ensure that the news-gathering process is free from government intrusion, allowing journalists to protect their sources and the information they collect in the course of their reporting. By affording legal protections over a journalist's work product, the PPA enables the media to function effectively as a check on government and other powerful institutions, thereby fostering a more informed public. The act aims to balance the necessity of law enforcement to obtain evidence in criminal investigations against the public interest in news reporting and freedom of the press. This foundational support for journalistic freedom emphasizes the importance of protecting the integrity of news reporting and the rights of individuals involved in the media process.

8. What federal privacy law contains specific requirements for how organizations must dispose of sensitive personal information?

A. FERPA

B. FACTA

C. GLBA

D. SOX

The Fair and Accurate Credit Transactions Act (FACTA) is indeed the federal privacy law that establishes specific requirements for the disposal of sensitive personal information. Under FACTA, organizations are mandated to take reasonable measures to protect against unauthorized access to or use of sensitive personal information in connection with the disposal of consumer reports or information derived from such reports. This is particularly important in preventing identity theft and safeguarding consumer privacy. FACTA includes provisions that require organizations to properly destroy or dispose of consumer information in a way that it cannot be reconstructed or read. This requirement reflects a growing concern over the security of personal data and the risks associated with improper disposal practices. While other laws listed, such as FERPA (Family Educational Rights and Privacy Act), GLBA (Gramm-Leach-Bliley Act), and SOX (Sarbanes-Oxley Act), deal with various aspects of privacy and data protection, they do not specifically focus on the disposal requirements of sensitive personal information to the same extent as FACTA does. Thus, when considering the context of disposing of sensitive information, FACTA is the most relevant and appropriate choice.

SAMPLE

9. Which law imposes specific requirements on the disposal of consumer report information?

A. Health Insurance Portability and Accountability Act (HIPAA)

B. Fair and Accurate Credit Transactions Act (FACTA)

C. Gramm-Leach-Bliley Act (GLBA)

D. Sarbanes-Oxley Act (SOX)

The Fair and Accurate Credit Transactions Act (FACTA) specifically addresses the disposal of consumer report information, establishing standards for how such data should be handled to prevent identity theft and ensure consumer privacy. Under FACTA, organizations are required to implement reasonable measures to protect against unauthorized access to or use of consumer information when disposing of it. This law essentially mandates that businesses and entities that handle consumer reports ensure that information is destroyed in a way that is irretrievably rendered unreadable and unusable. This legislation highlights the importance of safeguarding consumer data, particularly in an era where identity theft is a significant concern. By implementing disposal standards, FACTA aims to mitigate risks associated with improper or negligent disposal practices which could lead to information being accessed by unauthorized individuals. In contrast, the other laws mentioned do not specifically focus on the disposal of consumer report information, although they do cover various aspects of data privacy and consumer protection in different contexts. HIPAA is primarily concerned with the privacy and security of health information, the GLBA deals with the protection of consumers' personal financial information, and the Sarbanes-Oxley Act focuses on corporate accountability and financial disclosures, not directly addressing consumer report disposal.

10. Which U.S. federal law is most comparable to the EU's GDPR?

A. The Patriot Act

B. The Privacy Act

C. None

D. The Civil Rights Act

The most comparable U.S. federal law to the EU's General Data Protection Regulation (GDPR) would indeed be none of the options listed, as currently, there is no single U.S. federal law that mirrors the comprehensive scope and stringent requirements of the GDPR. The GDPR establishes a broad framework that includes principles of transparency, accountability, and individual rights regarding personal data, which encompasses a wide range of personal information and applies to both public and private entities. It mandates strict consent requirements, establishes the right to data portability, the right to be forgotten, and enforces significant penalties for non-compliance. While laws like the Privacy Act and the Civil Rights Act address certain aspects of privacy and data protection, they do not offer the same level of protection or broad applicability as the GDPR. The Privacy Act mainly governs how federal agencies handle personal data, and the Civil Rights Act is focused on preventing discrimination rather than protecting privacy rights in data handling. The lack of a single federal law that collectively addresses personal data protection in the U.S., akin to the GDPR, reinforces the idea that none of the options provided align closely enough with the comprehensive nature of the GDPR. Thus, asserting that none of the available choices are comparable to the GDPR is justified based on the

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://cipp.examzify.com

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

SAMPLE