CERTIFIED DOCUMENTATION INTEGRITY PRACTITIONER (CDIP) DOMIAN 6 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cdipdomain6.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. Which metrics are commonly used to monitor data integrity in health records?

A. Data accuracy, completeness, timeliness, consistency, number of integrity incidents, remediation time, and audit findings trends.

B. Number of patient visits.

C. System uptime.

D. Encryption strength.

2. What is the chain of custody in health records, and name a key control?

A. Documentation of custody and access from creation to destruction; key controls include tamper-evident seals and immutable audit logs

B. A process for archiving records after 5 years

C. A method for converting paper to digital records

D. A policy for patient consent forms

3. Which statement about non-repudiation in digital signatures is correct?

A. Non-repudiation is optional in most digital workflows.

B. Non-repudiation means encrypting all signatures.

C. Non-repudiation binds the signer's identity to the document content and prevents denial of authorship.

D. Non-repudiation allows any party to dispute the signer's involvement.

4. Which metric is typically used to gauge incident response effectiveness in a documentation integrity program?

A. Elapsed time to remediation.

B. Budget variance.

C. Number of employee trainings completed.

D. Customer satisfaction score.

5. On what date are HCPCS Level II updates released annually?

A. January 1

B. June 1

C. September 1

D. December 1

SAMPLE

6. On January 1st, which coding updates are released?

A. CPT and HCPCS Level 2

B. CPT only

C. ICD-10-CM/PCS and CPT

D. HCPCS Level 2 only

7. How does eDiscovery intersect with Domain 6 principles?

A. It requires preserving, collecting, and reviewing relevant electronically stored information while maintaining integrity, chain of custody, and defensible workflows.

B. It allows deleting irrelevant information to speed processing.

C. It ignores metadata to reduce complexity.

D. It only applies to paper records.

8. Which of the following best defines a data breach under HIPAA?

A. An impermissible use or disclosure of PHI; notification to affected individuals, the HHS, and sometimes the media, within required timeframes.

B. Any access to PHI by an employee, provided it is for treatment purposes.

C. A loss of PHI due to hardware failure that is encrypted.

D. A minor security incident that does not affect PHI integrity.

9. Which steps are included when managing litigation holds to preserve relevant PHI records?

A. Notify custodians only.

B. Identify scope and notify custodians.

C. Suspend deletions and implement monitoring.

D. Identify scope, notify custodians, suspend deletions, implement monitoring, and document preservation actions.

10. Which of the following is considered a technical safeguard?

A. Staff training

B. Audit controls

C. Limiting access

D. Workstation security

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which metrics are commonly used to monitor data integrity in health records?

A. Data accuracy, completeness, timeliness, consistency, number of integrity incidents, remediation time, and audit findings trends.

B. Number of patient visits.

C. System uptime.

D. Encryption strength.

Data integrity in health records is about keeping information accurate, complete, timely, and consistent across the system. The metrics that best capture this are data accuracy, completeness, timeliness, and consistency, together with counts of integrity incidents, remediation time, and trends in audit findings. Accuracy ensures the recorded values reflect the real patient facts; completeness ensures all required data are present; timeliness keeps information up-to-date; consistency ensures uniform data across different parts of the system. Tracking how often integrity incidents occur, how quickly issues are fixed, and how audit results trend over time shows both current performance and improvement over time. Choices focused on patient visits, system uptime, or encryption strength do not directly measure data quality: patient visits relate to volume of care, uptime relates to availability, and encryption strength relates to security rather than the data's accuracy, completeness, or consistency.

2. What is the chain of custody in health records, and name a key control?

A. Documentation of custody and access from creation to destruction; key controls include tamper-evident seals and immutable audit logs

B. A process for archiving records after 5 years

C. A method for converting paper to digital records

D. A policy for patient consent forms

Chain of custody in health records is the documented, traceable control of a record as it moves through its life—from creation to destruction. It ensures the integrity and authenticity of the information by recording who has custody, what access is granted, and what changes occur along the way, creating a reliable trail for clinical care and legal purposes. A key control is tamper-evident seals and immutable audit logs. Tamper-evident seals alert when a record has been opened or altered, signaling potential tampering. Immutable audit logs provide a nonchangeable record of every access and action taken on the record, including who accessed it and when, which enforces accountability and traceability throughout the record's lifecycle. Other options describe different concepts not focused on custody: archiving after a set period relates to retention, digitizing is about converting formats, and a policy for patient consent forms deals with consent, not the custody and control of the record.

SAMPLE

3. Which statement about non-repudiation in digital signatures is correct?

A. Non-repudiation is optional in most digital workflows.

B. Non-repudiation means encrypting all signatures.

C. Non-repudiation binds the signer's identity to the document content and prevents denial of authorship.

D. Non-repudiation allows any party to dispute the signer's involvement.

Non-repudiation in digital signatures is about creating verifiable proof that a specific person actually signed a particular document, and that the exact content of that document is what was signed. This binding is achieved by using the signer's private key to create the signature and a certificate that ties the signer's identity to that key, which others can verify with the public key. When a signature is validated, the combination of the signer's identity, the signed data, and the signature itself provides credible evidence of origin and authorship, making it difficult for the signer to deny having signed the document. It's not about encrypting signatures—the purpose of non-repudiation is not confidentiality of the signature but verifiable provenance. It's not typically described as optional in digital workflows where accountability is needed, and it doesn't enable broad disputes about involvement; rather, it aims to reduce disputes by providing solid, verifiable proof of who signed what.

4. Which metric is typically used to gauge incident response effectiveness in a documentation integrity program?

A. Elapsed time to remediation.

B. Budget variance.

C. Number of employee trainings completed.

D. Customer satisfaction score.

Measuring incident response effectiveness in a documentation integrity program focuses on how fast issues are detected and resolved. The best indicator is the elapsed time to remediation—the duration from when an incident is discovered to when it is fully remediated and closed. This metric captures the speed and efficiency of the entire response cycle, including detection, containment, remediation, and verification, and directly affects how long the organization operates with compromised or unreliable documentation. Shorter remediation times signal a more effective incident response capability and a more resilient documentation environment. Other options—budget variance, training counts, or customer satisfaction—measure cost control, preparedness, or external perception, but they don't directly reflect how quickly and effectively incidents are handled.

5. On what date are HCPCS Level II updates released annually?

A. January 1

B. June 1

C. September 1

D. December 1

The annual HCPCS Level II updates are released on January 1. This date is the standard release and effective date, so new codes, changes, and deletions are in place for the start of the calendar year. The other dates listed are not the official release date for the annual update, which is why January 1 is the correct choice.

SAMPLE

6. On January 1st, which coding updates are released?

A. CPT and HCPCS Level 2

B. CPT only

C. ICD-10-CM/PCS and CPT

D. HCPCS Level 2 only

At the start of the year, the coding updates released are CPT and HCPCS Level II. CPT codes, published by the American Medical Association, describe procedures and services, while HCPCS Level II codes cover items and services not included in CPT, such as supplies, equipment, and some drugs. Both code sets publish annual updates that take effect January 1, including new codes and changes to existing ones. ICD-10-CM/PCS updates follow a different schedule and are released on October 1, not January 1. So, the January 1 releases you'd encounter are CPT and HCPCS Level II.

7. How does eDiscovery intersect with Domain 6 principles?

A. It requires preserving, collecting, and reviewing relevant electronically stored information while maintaining integrity, chain of custody, and defensible workflows.

B. It allows deleting irrelevant information to speed processing.

C. It ignores metadata to reduce complexity.

D. It only applies to paper records.

In eDiscovery, the goal is to preserve and handle electronic information so it stays intact and defensible for legal proceedings. Domain 6 emphasizes maintaining data authenticity, traceability, and repeatable, defensible processes throughout the lifecycle. The best option captures this by describing the need to preserve, collect, and review relevant electronically stored information while keeping data integrity, chain of custody, and defensible workflows intact. Deleting irrelevant information contradicts the preservation mindset and can risk sanctions; ignoring metadata loses crucial context about authorship, timing, and provenance; and suggesting it only applies to paper records is incorrect because eDiscovery centers on electronic data, with paper records often relevant only as a subset.

SAMPLE

8. Which of the following best defines a data breach under HIPAA?

A. An impermissible use or disclosure of PHI; notification to affected individuals, the HHS, and sometimes the media, within required timeframes.

B. Any access to PHI by an employee, provided it is for treatment purposes.

C. A loss of PHI due to hardware failure that is encrypted.

D. A minor security incident that does not affect PHI integrity.

HIPAA defines a data breach as an impermissible use or disclosure of protected health information (PHI) that compromises the privacy or security of the PHI. That means not every security hiccup counts as a breach—only when someone not allowed to access or share PHI does so in a way that compromises its privacy or security. For example, an employee accessing PHI for legitimate treatment is permitted and not a breach, and a loss of PHI that's encrypted typically isn't considered a breach because the information remains protected. If a breach occurs, the entity responsible must issue notices to the people affected, to the Department of Health and Human Services, and, in certain cases, to the news media, within required timeframes. The notification to individuals is generally required without unreasonable delay and no later than about 60 days after discovery. HHS must be notified within the same general timeframe, with media notification required for larger breaches that affect a substantial number of individuals in a given area. This combination of defining what constitutes a breach and outlining who must be notified—within specific timeframes—is what makes the choice the best answer. A minor security incident that doesn't affect PHI, or a loss of PHI when the data remains encrypted, do not meet the breach criteria, so they don't trigger the same notification requirements.

9. Which steps are included when managing litigation holds to preserve relevant PHI records?

A. Notify custodians only.

B. Identify scope and notify custodians.

C. Suspend deletions and implement monitoring.

D. Identify scope, notify custodians, suspend deletions, implement monitoring, and document preservation actions.

Managing a litigation hold for PHI hinges on a complete, defensible preservation process that keeps relevant data intact for discovery. Start by identifying the scope: determine which PHI records, data sources, custodians, and time frames may be relevant, so the hold targets the right information without missing pieces or sweeping too broadly. Next, notify custodians: clearly communicate the hold to those who manage or access PHI and spell out their obligation to preserve data as it currently exists. Then suspend deletions: pause automatic purges and any data lifecycle actions on the identified materials and systems to prevent loss or alteration. Implement monitoring: establish controls to verify compliance, track preservation actions, and catch any deviations or attempted deletions, with an audit trail. Finally, document preservation actions: maintain a thorough record of the scope, notifications, actions taken, systems involved, dates, and rationale to support defensibility and future review. This combination ensures PHI remains preserved throughout the legal process and meets regulatory and ethical obligations; partial steps would leave gaps that could undermine the hold and potential discovery.

SAMPLE

10. Which of the following is considered a technical safeguard?

A. Staff training

B. Audit controls

C. Limiting access

D. Workstation security

Technical safeguards are technology-based protections that guard electronic PHI. Audit controls are a clear example because they rely on the information system itself to automatically log, monitor, and analyze activities related to PHI. This creates an electronic trail showing who accessed data, when, and what actions were taken, which is essential for detecting misuse and guiding incident response. Staff training, by contrast, is an administrative safeguard, focusing on policies and procedures rather than automated system monitoring. Workstation security is a physical safeguard, addressing the protection of devices and their use. Limiting access describes restricting who can reach data and is typically carried out through access controls; while related to technical measures, the defining feature of a technical safeguard is the use of automated, system-wide auditing and monitoring, which is why audit controls are the best fit here.

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://cdipdomain6.examzify.com

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

SAMPLE