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

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. What are tamper-evident controls and give two examples?

A. Regular backups without audit features.

B. Encrypting entire documents for confidentiality.

C. Assigning random identifiers to files.

D. Mechanisms that reveal any unauthorized modification; examples include immutable audit logs and write-once or append-only storage.

2. Which mechanism is commonly used to legally transfer PHI data across borders?

A. Standard Contractual Clauses (SCCs)

B. Public access to data.

C. Single-user license

D. Mandatory data anonymization only

3. Why are independent verification and dual control important?

A. They slow processes and hinder compliance.

B. They reduce risk of fraud or error by requiring separate individuals to perform or approve critical integrity actions.

C. They are optional and unnecessary for governance.

D. They apply only to financial data.

4. Which term describes the intentional and mistaken misrepresentation of reimbursement claims submitted to government-sponsored health programs?

A. Fraud and abuse

B. Billing errors

C. Reimbursement misrepresentation

D. Health care misreporting

5. What is the primary purpose of defensible disposal in records management?

A. To maximize the amount of data retained for as long as possible.

B. To ensure records are destroyed without any evidence of the process.

C. To dispose of records securely with documentation to demonstrate compliant and defensible actions.

D. To move all records to offsite storage indefinitely.

6. Which of the following is considered a hot topic in compliance?

A. Repeated provider errors

B. Annual code updates

C. Reimbursement changes

D. All of the above

7. After a data migration, which activity verifies that the migrated data maintains original metadata and provenance?

A. Reconciliation and integrity checks against source

B. Deleting source data

C. Re-encoding all files to a new format without checks

D. Ignoring provenance due to efficiency

8. On what date are ICD-10-CM/PCS updates released annually?

A. October 1

B. January 1

C. July 1

D. December 1

9. A _____ is a communication tool or process used to clarify documentation in the health record.

A. Query

B. Progress note

C. H&P

D. Discharge summary

10. Which government department coordinates fraud and abuse control along with the Office of Inspector General (OIG)?

A. Department of Justice

B. Centers for Medicare & Medicaid Services

C. Department of Health and Human Services

D. Federal Trade Commission

Answers

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

Explanations

1. What are tamper-evident controls and give two examples?

A. Regular backups without audit features.

B. Encrypting entire documents for confidentiality.

C. Assigning random identifiers to files.

D. Mechanisms that reveal any unauthorized modification; examples include immutable audit logs and write-once or append-only storage.

Tamper-evident controls are mechanisms that ensure any unauthorized modification to data or logs leaves a detectable trace, so you can prove that changes did or did not occur after the fact. They create a trustworthy record of actions and make it possible to notice if someone tampered with information. Two clear examples are immutable audit logs and write-once or append-only storage. Immutable audit logs are designed so once an entry is written, it cannot be altered or deleted; cryptographic protections and strict access controls maintain the integrity and provide a verifiable history of events. Write-once or append-only storage allows only additions to the data; existing records cannot be edited or erased, which preserves a tamper-evident trail of all stored information. Together, these controls help with accountability, forensic analysis, and compliance by making tampering detectable. Regular backups without audit features don't inherently show tampering, encryption protects confidentiality rather than detect changes, and simply assigning random identifiers to files doesn't provide a mechanism to reveal unauthorized modifications.

2. Which mechanism is commonly used to legally transfer PHI data across borders?

A. Standard Contractual Clauses (SCCs)

B. Public access to data.

C. Single-user license

D. Mandatory data anonymization only

When PHI moves across borders, you need a legally binding framework that obligates the receiving party to protect the data just as you would at home. Standard Contractual Clauses provide that framework: they are pre-approved contract terms used between the data exporter and data importer to ensure adequate data protection, covering how the data is processed, secured, and safeguarded, how breach notices are handled, how subprocessor activities are controlled, and how data subjects can exercise their rights. This mechanism is widely recognized because it creates an enforceable, auditable set of obligations specifically for cross-border transfers, and it can be updated to stay aligned with evolving privacy laws. In contrast, public access to data would compromise confidentiality, a single-user license is about software rights rather than data protection, and mandatory data anonymization alone isn't always sufficient to enable cross-border transfers when there remains a risk of re-identification. So Standard Contractual Clauses are the standard method used to legally transfer PHI data across borders.

3. Why are independent verification and dual control important?

A. They slow processes and hinder compliance.

B. They reduce risk of fraud or error by requiring separate individuals to perform or approve critical integrity actions.

C. They are optional and unnecessary for governance.

D. They apply only to financial data.

Independent verification and dual control center on separating duties and adding oversight for actions that affect data integrity. The key idea is to prevent a single person from both carrying out and approving a critical task, which creates an opportunity for fraud or mistakes to go unnoticed. Dual control requires two people to participate in an action or its approval, so no one can unilaterally push through changes. Independent verification involves an outside or separate reviewer checking results, updates, or decisions to confirm accuracy and completeness. This combination strengthens governance by creating accountability and an auditable trail. For example, someone might perform a sensitive data change, but another person or team must approve or review the change before it takes effect. This reduces the chance that errors slip through or that fraudulent activity goes undetected. While these controls may slow processes, they are a deliberate trade-off that enhances integrity and compliance across processes, not just financial ones. Other options miss the point: these controls are not merely about slowing workflows, they are not optional in robust governance, and they apply to more than just financial data, extending to any critical actions that affect data or system integrity.

4. Which term describes the intentional and mistaken misrepresentation of reimbursement claims submitted to government-sponsored health programs?

A. Fraud and abuse

B. Billing errors

C. Reimbursement misrepresentation

D. Health care misreporting

Misrepresentation of claims to government health programs is described as fraud and abuse because it covers both intentional deception and improper billing practices that can lead to improper payments. Fraud refers to knowingly submitting false statements or misrepresenting facts to obtain payment, while abuse encompasses improper or unsound billing practices that aren't necessarily criminal but still misuse program funds. This combined term is the standard label used in Medicare/Medicaid oversight and enforcement to capture a range of improper activities, from billing for services not provided to upcoding or upbilling for higher reimbursements. The other options don't reflect the accepted terminology for this broad issue.

5. What is the primary purpose of defensible disposal in records management?

A. To maximize the amount of data retained for as long as possible.

B. To ensure records are destroyed without any evidence of the process.

C. To dispose of records securely with documentation to demonstrate compliant and defensible actions.

D. To move all records to offsite storage indefinitely.

Defensible disposal is about ending the lifecycle of records in a way that is secure, controlled, and clearly verifiable. The key idea is that destruction isn't random or overdue; it follows a approved retention schedule and is performed in a manner appropriate to the data's sensitivity. What makes it defensible is the documentation that accompanies the disposal—dates, what was destroyed, how it was destroyed, who authorized it, and who conducted the destruction. That records trail lets an auditor or regulator see exactly what happened and confirm that the organization complied with policy, legal holds, and privacy requirements. It also reduces risk by ensuring obsolete information is removed responsibly, freeing up space and lowering the chance of a breach from keeping data longer than needed. Choosing to maximize retention misses the point of defensible disposal, because it prioritizes keeping data over disciplined lifecycle management. Destroying records without any evidence fails the defensible standard because there's no proof that the action was authorized or compliant. Moving everything offsite indefinitely isn't disposal at all; it's a storage decision that delays the proper end-of-life process and doesn't provide the documented basis needed to defend the action.

6. Which of the following is considered a hot topic in compliance?

A. Repeated provider errors

B. Annual code updates

C. Reimbursement changes

D. All of the above

Hot topics in compliance are areas that carry ongoing risk and demand active oversight. Repeated provider errors point to gaps in documentation, coding, or clinical practice that can trigger investigations, remediation, or sanctions if not addressed. Annual code updates require staying current with coding sets (like ICD, CPT, HCPCS) because using outdated codes can lead to incorrect billing and compliance violations. Reimbursement changes reflect evolving payer policies and medical necessity criteria, which necessitate updates to policies, training, and denials management to maintain billing integrity. Since each of these areas regularly attracts regulatory and payer scrutiny, they're all considered hot topics. That's why the best choice is all of the above.

7. After a data migration, which activity verifies that the migrated data maintains original metadata and provenance?

A. Reconciliation and integrity checks against source

B. Deleting source data

C. Re-encoding all files to a new format without checks

D. Ignoring provenance due to efficiency

Ensuring metadata and provenance survive a data migration requires comparing the migrated data to the original source and performing checks that verify both content and descriptive information. This involves reconciliation and integrity checks that confirm the migrated copies are faithful to the originals: the data bits match, the checksums align, and metadata fields (such as creation date, origin, and any provenance records) are preserved and correctly mapped. By systematically validating these aspects, you establish that the migration did not alter or lose essential context about the data's origins and history, which is crucial for trust, authenticity, and long-term preservation. Deleting source data would eliminate the basis for verification and break the provenance trail. Re-encoding all files to a new format without any checks removes the safeguards that ensure metadata and provenance are preserved and verifiable. Ignoring provenance altogether ignores critical historical context that supports trust and accountability in the data lifecycle.

8. On what date are ICD-10-CM/PCS updates released annually?

A. October 1

B. January 1

C. July 1

D. December 1

Updates to ICD-10-CM diagnosis codes and ICD-10-PCS procedure codes are issued once a year and take effect with the start of the U.S. government's fiscal year on October 1. This timing means new, modified, or deleted codes are released for use in the upcoming year starting October 1, aligning billing, documentation, and claims processes with the new code sets. The other dates don't align with this annual adoption cycle, so they aren't the standard release date.

9. A _____ is a communication tool or process used to clarify documentation in the health record.

A. Query

B. Progress note

C. H&P

D. Discharge summary

A query is a formal communication used to obtain clarification about documentation in the health record. In clinical documentation integrity, when the coder encounters documentation that is ambiguous, incomplete, or potentially conflicting, they issue a query to the treating clinician. The clinician's response helps ensure the coded diagnoses and procedures truly reflect what happened during the patient's care, supporting accurate codes and appropriate reimbursement. A progress note records ongoing care and daily events, not a mechanism to clarify chart entries. An H&P is the initial History and Physical assessment, not a clarification tool. A discharge summary summarizes the hospital stay and final status at discharge, not a process for resolving documentation questions. For example, if the chart mentions pneumonia but lacks details on acuity or whether it's definite versus suspected, a query asks the clinician to confirm the precise diagnosis and its documentation, enabling correct coding.

10. Which government department coordinates fraud and abuse control along with the Office of Inspector General (OIG)?

A. Department of Justice

B. Centers for Medicare & Medicaid Services

C. Department of Health and Human Services

D. Federal Trade Commission

Working together to fight fraud and abuse in health programs relies on pairing the investigative work of the Office of Inspector General with the enforcement authority of a separate department. The OIG conducts audits and investigations to uncover improper billing, kickbacks, and other fraudulent activity. When a case involves potential criminal conduct or civil violations, the OIG partners with the Department of Justice to prosecute offenders and pursue enforcement actions. This collaboration ensures that detection leads to real accountability, with OIG handling the findings and DOJ handling the prosecutorial side. Other options either administer programs (like CMS), sit within the same department (HHS) but aren't the enforcement partner for investigations led by the OIG, or focus on different areas of consumer protection. The Department of Justice is the department that coordinates fraud and abuse control with the OIG.

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!