Introduction to the Fundamentals of Law for Health Information and Information Management Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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 is the legal term used to describe the physical and electronic protection of health information?

A. Access

B. Confidentiality

C. Privacy

D. Security

2. What term describes the ability to exchange electronic health information across organizations using nationally recognized interoperability standards?

A. Data encryption

B. Interoperability

C. Data governance

D. Data replication

3. The totality of safeguards including hardware, software, personnel policies, information practice policies, disaster preparedness, and oversight is called what?

A. System security

B. Health information governance

C. Physical security

D. Data integrity

4. Stewardship is a component of which framework?

A. Risk management

B. Privacy program

C. Data quality

D. Information governance

5. Which of the following is a primary purpose of data security?

A. To increase data sharing

B. To protect data from unauthorized access and alteration

C. To ensure data is always public

D. To reduce data storage

6. Which statement best describes the relationship between HIPAA and HITECH?

A. HIPAA predates HITECH and HITECH broadens protections

B. HITECH replaces HIPAA

C. They are unrelated

D. HIPAA was created after HITECH

7. Which term describes electronic documents that include information about the document or file that can be used to store and retrieve later?

A. Metadata

B. Edition

C. Header

D. Content tags

8. Which term refers to an electronic health record that can be created, managed, and consulted across more than one healthcare organization?

A. Electronic Health Record

B. Electronic Medical Record

C. Hybrid Health Record

D. Health Information Exchange

9. Privileged communication is usually delineated by which level of law?

A. Federal law

B. State law

C. Local ordinances

D. International law

10. According to ASTM E31 Health Informatics, security is defined from how many perspectives?

A. One

B. Two

C. Three

D. Four

Answers

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

Explanations

1. What is the legal term used to describe the physical and electronic protection of health information?

A. Access

B. Confidentiality

C. Privacy

D. Security

Security is the term that describes protecting health information through safeguards in both physical and electronic forms. It covers measures like locked facilities, limited access, and surveillance for physical protection, as well as access controls, authentication, encryption, and audit trails for electronic protection. Under HIPAA, the Security Rule specifically focuses on these safeguards to shield electronic PHI, while privacy concerns the individual's rights over how information is used and disclosed, and confidentiality refers to keeping information secret from unauthorized parties. Access is about who can view data, not the protective measures themselves. So the protection of health information in both realms is best described as security.

2. What term describes the ability to exchange electronic health information across organizations using nationally recognized interoperability standards?

A. Data encryption

B. Interoperability

C. Data governance

D. Data replication

Interoperability is the ability to exchange electronic health information across organizations using nationally recognized interoperability standards. It means that different health IT systems can not only send data to each other but also interpret and use that data meaningfully. This relies on two layers: technical standards that specify how data is formatted and transmitted (such as HL7 and FHIR for messages, DICOM for imaging) and semantic standards that ensure the terms and codes have the same meaning across systems (like SNOMED CT, LOINC, and ICD-10). When these standards are in place, information can flow between providers, pharmacies, labs, and other partners in a way that supports accurate understanding and continuity of care. Data encryption protects information during transfer, but it does not address whether systems can exchange and interpret data. Data governance covers policies and stewardship, and data replication is about creating copies of data—neither captures the cross-organizational exchange powered by standardized interoperability.

3. The totality of safeguards including hardware, software, personnel policies, information practice policies, disaster preparedness, and oversight is called what?

A. System security

B. Health information governance

C. Physical security

D. Data integrity

System security is the comprehensive protective framework for information systems, covering both the technology and the people and processes that run it. It includes safeguards at the hardware and software levels, as well as the personnel policies, information-use policies, disaster preparedness, and governance oversight that together protect the confidentiality, availability, and integrity of data. This broad approach ensures that access is controlled, data remains accurate, and operations can continue despite disruptions. Health information governance deals with managing health information across its lifecycle and ensuring privacy, quality, and accountability; it's broader than just security controls. Physical security focuses on protecting physical assets like servers and facilities, but doesn't fully address the software, policies, and disaster planning aspect. Data integrity concerns the accuracy and consistency of data, which is part of security but not the entire protective framework.

4. Stewardship is a component of which framework?

A. Risk management

B. Privacy program

C. Data quality

D. Information governance

Stewardship sits within information governance. In this framework, stewardship means designating data stewards who are accountable for specific data assets and for enforcing policies, standards, and controls across the organization. These stewards own data quality, metadata, access, security, and lifecycle decisions, ensuring that data is accurate, usable, protected, and compliant with laws and business requirements. By providing clear responsibility and oversight, stewardship operationalizes governance, linking people, processes, and technology to manage information as a valuable asset. While risk management focuses on reducing risks and a privacy program on protecting personal data, stewardship is the governance role that coordinates and enforces broader data management responsibilities, including data quality and privacy practices.

5. Which of the following is a primary purpose of data security?

A. To increase data sharing

B. To protect data from unauthorized access and alteration

C. To ensure data is always public

D. To reduce data storage

Data security is about keeping information safe from people who shouldn't access it and from changes that aren't authorized. In health information management, this means protecting patient records so they remain private, accurate, and available to those who need them. Controls like access limits, encryption, audit logs, and backups help ensure that only authorized users can view or alter data, that any changes are tracked, and that records aren't corrupted or lost. The goal isn't to increase sharing, reveal data publicly, or reduce storage; it's to safeguard confidentiality and integrity while preserving reliable access for legitimate use.

6. Which statement best describes the relationship between HIPAA and HITECH?

A. HIPAA predates HITECH and HITECH broadens protections

B. HITECH replaces HIPAA

C. They are unrelated

D. HIPAA was created after HITECH

HIPAA sets the baseline for protecting health information, and HITECH builds on it rather than replacing it. HIPAA, enacted in 1996, established national standards for protecting privacy and securing health data. HITECH, introduced in 2009 as part of the stimulus legislation, strengthens those protections by expanding requirements to business associates, increasing penalties for violations, and introducing breach notification rules. Because HITECH came after HIPAA and reinforces and broadened its protections, the relationship is that HITECH broadens HIPAA's reach and enforcement, not that it replaces HIPAA or that they are unrelated.

7. Which term describes electronic documents that include information about the document or file that can be used to store and retrieve later?

A. Metadata

B. Edition

C. Header

D. Content tags

Metadata is data about a document that describes its characteristics and context, making storage, organization, and retrieval possible later. It includes details such as who created the file, when it was created or last modified, the file type, size, and any keywords or topics associated with it. This descriptive layer lets health information managers index and locate records across systems, link related records, and apply appropriate privacy and retention rules. An edition refers to a specific version or revision of a document, not the broader set of descriptive information used to find and manage the file. A header is the content that appears at the top of a page, not the information about the document as a whole. Content tags are specific keywords or labels, which are part of metadata, but the term that covers the overall descriptive information used to store and retrieve documents is metadata.

8. Which term refers to an electronic health record that can be created, managed, and consulted across more than one healthcare organization?

A. Electronic Health Record

B. Electronic Medical Record

C. Hybrid Health Record

D. Health Information Exchange

The ability to create, manage, and consult a patient's record across multiple healthcare organizations is characteristic of an Electronic Health Record. An Electronic Health Record is designed for interoperability, sharing a longitudinal view of a patient's information across different providers and settings. An Electronic Medical Record, by contrast, is typically a digital version of the chart kept within a single organization and isn't inherently built for cross-organization access. A Health Information Exchange is the network and set of standards that enables these records to be shared securely between organizations, rather than describing the record itself. A Hybrid Health Record isn't a standard term for cross-organizational access. So the term that fits cross-organization use best is Electronic Health Record.

9. Privileged communication is usually delineated by which level of law?

A. Federal law

B. State law

C. Local ordinances

D. International law

Privilege in this context means protections that keep certain confidential communications from being disclosed in court. The rules that determine what counts as privileged, who can assert it, and how broad the protection is are set by law at the state level, through statutes and common-law decisions. This is why state law is the usual source for delineating privileged communications—the policies about confidentiality in professional relationships (like doctor–patient or attorney–client) are historically rooted in state law and vary from one state to another. Federal law does regulate some privileges in federal cases, but there isn't a single nationwide framework that overrides state definitions in most situations. Local ordinances don't establish these general evidentiary protections, and international law doesn't govern domestic privilege. So the best answer is that privilege is usually delineated by state law.

10. According to ASTM E31 Health Informatics, security is defined from how many perspectives?

A. One

B. Two

C. Three

D. Four

Security in health informatics is viewed from two perspectives: confidentiality and integrity. Confidentiality means protecting patient information from unauthorized access, preserving privacy and the right to control who sees data. Integrity means keeping information accurate and unaltered, ensuring that data remain trustworthy and reliable for clinical decisions. While availability is important for access to information, the ASTM E31 framework emphasizes these two aspects to ensure both privacy and trust in health records.

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://introtofundoflawforinfomgmt.examzify.com

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