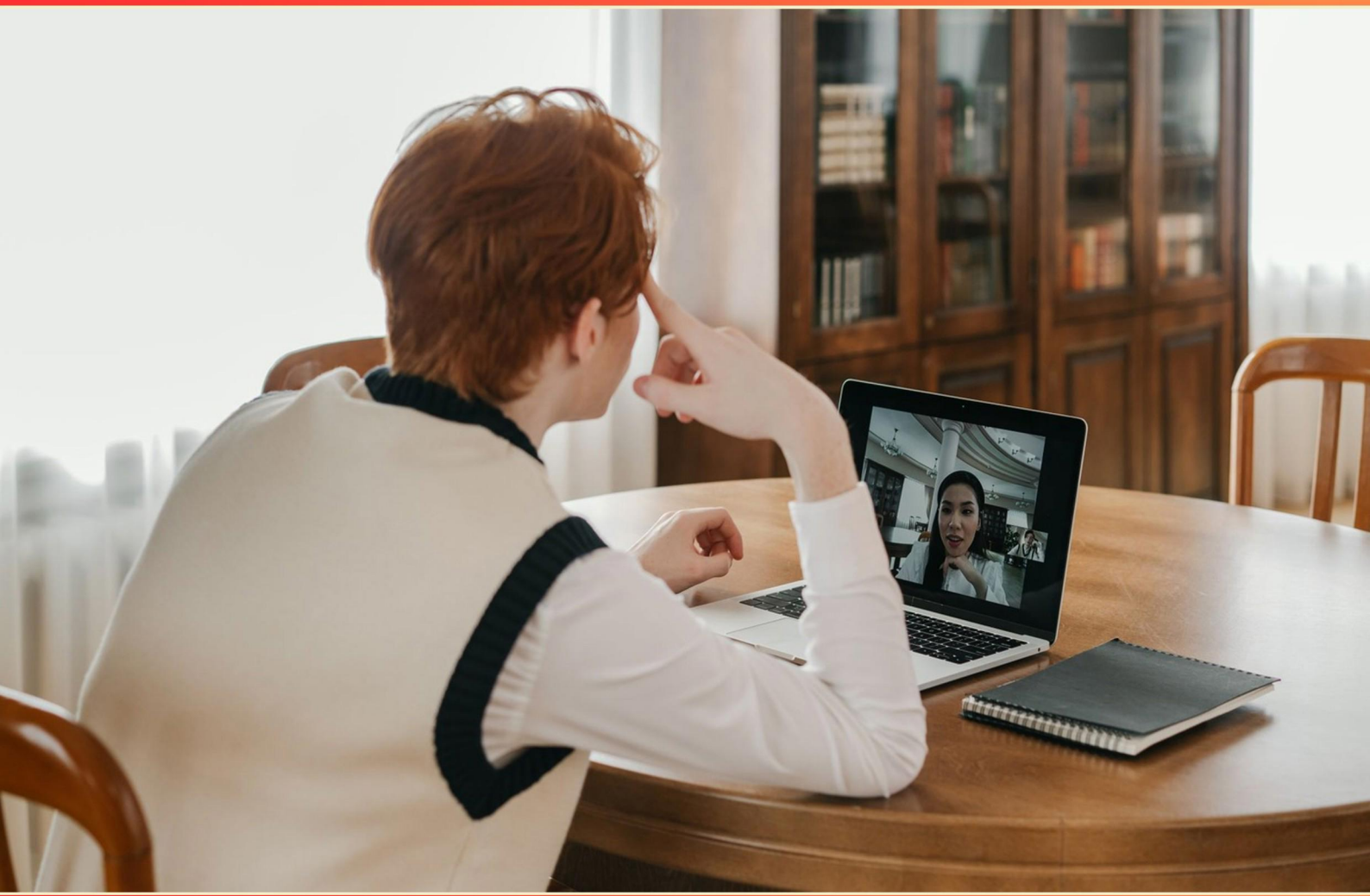
BOARD CERTIFIED–TELEMENTAL HEALTH PROVIDER (BC-TMH) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://bctmh.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. The duty to warn is generally derived from Tarasoff v. Regents and related ethical standards and state laws. Which statement best describes its basis?

A. Tarasoff decisions and professional ethical standards

B. Federal statute

C. Patient consent forms

D. Financial risk management policies

2. A video teleconferencing codec is used to do what?

A. Encrypt data at rest

B. Encode and decode and compress and transmit audio and video data

C. Route network packets

D. Authenticate users

3. Which factor is explicitly listed as an ethical consideration when selecting telehealth technology?

A. Verification of identity

B. The device brand name

C. The client's data plan

D. The interface color scheme

4. Which term describes carrying private communications over the public Internet using tunneling or port forwarding?

A. Virtual Private Network

B. Wide Area Network

C. Local Area Network

D. Wireless Fidelity

5. Node in this context is defined as what?

A. An endpoint

B. A router

C. A hub

D. A firewall

6. Which statement about billing and payment considerations in telehealth is accurate?

A. Billing should track insurance claims and reasons for denial

B. Billing should be based solely on session length

C. Billing is never required in telehealth

D. Billing only uses cash payments

7. Which term refers to the format proposed in the H.261 standard for standardizing video resolutions, also known as FCIF or CIF?

A. EDI

B. EPR

C. EMR

D. Full Common Intermediate Format (FCIF or CIF)

8. Does HIPAA require a mental health provider to inform a patient before sharing PHI to prevent or lessen a serious or imminent threat?

A. Not at the time of disclosure; the Notice of Privacy Practices should include an example; exceptions exist for abuse reporting.

B. Yes, always before disclosure.

C. Only if the patient is present.

D. Only if the patient signs a release.

9. If a client is not a fit for your service, what should you do?

A. Ignore the inquiry

B. Create a clear policy beforehand to know how to respond; let them know they are not a fit and why; provide referrals, provide the client written notice and referrals, and document this process

C. Provide referrals but do not document

D. Charge for consultation

10. What does the abbreviation MP stand for when describing a unit of image resolution, equal to one million pixels?

A. Megapixel

B. MPEG

C. MP3

D. Multiplexer

Answers

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

Explanations

1. The duty to warn is generally derived from Tarasoff v. Regents and related ethical standards and state laws. Which statement best describes its basis?

A. Tarasoff decisions and professional ethical standards

B. Federal statute

C. Patient consent forms

D. Financial risk management policies

The duty to warn comes from a court decision and from professional ethics, not from federal law or administrative forms. Tarasoff v. Regents of the University of California established that clinicians have an obligation to protect individuals who are being threatened by a patient, which can include warning the potential victim or taking other steps to prevent harm. Professional ethical standards, such as those issued by psychology and psychiatry associations, reinforce this protective obligation and guide how to respond to credible threats. In practice, many states have codified this duty in statutes, but it begins with the Tarasoff ruling and ethical expectations, not federal statutes or unrelated policies. Patient consent forms address confidentiality and consent, not the clinician's duty to warn, and financial risk management policies deal with organizational risk rather than clinical duties to protect third parties.

2. A video teleconferencing codec is used to do what?

A. Encrypt data at rest

B. Encode and decode and compress and transmit audio and video data

C. Route network packets

D. Authenticate users

A video teleconferencing codec handles transforming raw media into a compact, streamable form and then turning it back into playable media. It encodes the incoming audio and video, compresses the data to fit network bandwidth, and then transmits the compressed bitstream. On the receiving end, it decodes and decompresses the stream for playback. This focus on converting and optimizing media for transmission makes it clear why encoding, decoding, and compression with transmission are the codec's primary roles. Rout-ing network packets is handled by routing devices, not by the codec. Encrypting data at rest and authenticating users are security and identity tasks, typically outside the codec's scope.

3. Which factor is explicitly listed as an ethical consideration when selecting telehealth technology?

A. Verification of identity

B. The device brand name

C. The client's data plan

D. The interface color scheme

Verifying the patient's identity is essential because it directly protects confidentiality and ensures the right person is receiving and contributing to the care. In telehealth, confirming who you're talking to prevents unauthorized access to sensitive health information and helps ensure that notes, diagnoses, and treatment decisions are linked to the correct individual. This aligns with ethical duties to safeguard privacy and with legal expectations for authenticating patients in virtual settings. The other factors—such as the device brand, the patient's data plan, or the interface color—don't inherently address these privacy and safety obligations, though they can influence usability or access, they aren't explicit ethical requirements for selecting telehealth technology.

4. Which term describes carrying private communications over the public Internet using tunneling or port forwarding?

A. Virtual Private Network

B. Wide Area Network

C. Local Area Network

D. Wireless Fidelity

Creating a secure private channel over the public Internet via tunneling is what a virtual private network does. A VPN wraps your traffic in encryption and encapsulation, sending it through the public Internet as if it were part of a private network. Tunneling protocols handle the encapsulation, forming a secure tunnel between your device and the VPN server, while port forwarding can direct traffic from the client into the VPN gateway to reach internal resources. This arrangement protects data from eavesdroppers and lets remote users access internal networks as if they were on-site. By contrast, a wide area network covers broad geographic areas, a local area network stays within a small area like a building, and Wireless Fidelity refers to Wi Fi technology, not the private tunnel mechanism.

5. Node in this context is defined as what?

A. An endpoint

B. A router

C. A hub

D. A firewall

In this context, a node refers to the endpoint device—the device at the edge that the user interacts with to send and receive data, such as a computer, tablet, or smartphone used by patient or clinician. These are the actual end points of the telehealth session. The other options describe network infrastructure that moves or safeguards traffic (router, hub, firewall) rather than the user-facing devices, so they aren't the intended meaning of a node here.

6. Which statement about billing and payment considerations in telehealth is accurate?

A. Billing should track insurance claims and reasons for denial

B. Billing should be based solely on session length

C. Billing is never required in telehealth

D. Billing only uses cash payments

In telehealth, managing how you get paid is a key part of the workflow. Tracking insurance claims and the reasons they're denied helps you understand payer patterns, ensure you're coding and documenting services correctly, and identify where you need to adjust processes or documentation to get reimbursed. By monitoring denials, you can appeal appropriately, verify patient eligibility, and align your billing with payer policies and telehealth rules (such as allowable modalities and locations). This approach supports revenue integrity and helps prevent revenue leakage. Billing should not be based solely on session length, since reimbursement often depends on the specific service code, time rules, and payer policies, including telehealth modifiers and eligibility. Billing is not never required—services typically require billing to obtain payment. Billing does not rely only on cash payments; while cash is possible, many payers require claims to be submitted for reimbursement, and a system-wide approach to billing covers all payment sources.

7. Which term refers to the format proposed in the H.261 standard for standardizing video resolutions, also known as FCIF or CIF?

A. EDI

B. EPR

C. EMR

D. Full Common Intermediate Format (FCIF or CIF)

In H.261, the aim is to standardize how large the video frames are so different devices can encode and decode consistently. The format name used for this standardized resolution family is the Common Intermediate Format, CIF, with the "full" variant FCIF sometimes used to emphasize the higher end of that format. This term directly reflects the standardization approach H.261 uses for video resolutions, making Full Common Intermediate Format (FCIF or CIF) the best description of the format in question. The other acronyms listed (EDI, EPR, EMR) refer to unrelated concepts in other fields and do not describe video resolution formats in H.261.

8. Does HIPAA require a mental health provider to inform a patient before sharing PHI to prevent or lessen a serious or imminent threat?

A. Not at the time of disclosure; the Notice of Privacy Practices should include an example; exceptions exist for abuse reporting.

B. Yes, always before disclosure.

C. Only if the patient is present.

D. Only if the patient signs a release.

Disclosures to prevent a serious or imminent threat are permitted under HIPAA without patient authorization or prior notice. The Privacy Rule allows sharing necessary PHI to prevent harm to a specific individual or the public, so you're not required to obtain the patient's consent or inform them before making the disclosure. The Notice of Privacy Practices should describe the kinds of disclosures that may occur without consent, including examples of threat-related situations, and there are legal justifications for abuse reporting under applicable laws. In practice, you document the rationale and limit the disclosure to the minimum necessary information, and you may inform the patient afterward if appropriate and feasible. The other options imply that pre-disclosure consent, patient presence, or a signed release are needed, which is not how the imminent-threat disclosure rule works.

9. If a client is not a fit for your service, what should you do?

A. Ignore the inquiry

B. Create a clear policy beforehand to know how to respond; let them know they are not a fit and why; provide referrals, provide the client written notice and referrals, and document this process

C. Provide referrals but do not document

D. Charge for consultation

The central idea here is having a pre-established, written policy for handling inquiries that aren't a good fit, and following it consistently. This approach supports ethical practice, clear communication, and good clinical governance. When a client isn't a fit, you should respond promptly and clearly: let them know that their situation isn't within your service scope, explain why in a respectful, nonjudgmental way, and provide appropriate referrals to other options or levels of care. Offering written notice helps ensure the client understands the rationale and the next steps, while documenting the entire process creates a record of what was discussed, the reasons for the decision, and the referrals made. This combination protects the client's rights, supports their access to suitable care, and provides accountability for the clinician. Having this policy in place beforehand reduces guesswork during inquiries and aligns with ethical obligations in telepsychiatry and telepsychology, including transparency, informed consent, and appropriate boundaries. It also helps you manage risk and ensures consistency across cases. Ignoring the inquiry is inappropriate because it withholds information and a potential path to care. Providing referrals without documentation lacks a clear record of the rationale and steps taken, which can create confusion and accountability gaps. Charging for a consultation when you're not delivering service is not appropriate or fair to the client.

10. What does the abbreviation MP stand for when describing a unit of image resolution, equal to one million pixels?

A. Megapixel

B. MPEG

C. MP3

D. Multiplexer

MP stands for megapixel, a unit used to describe image resolution in terms of millions of pixels. The prefix mega- means one million, so a single megapixel equals one million pixels. In cameras and image sensors, resolution is often stated in megapixels (for example, 12 MP means about 12 million pixels) because it captures how much detail the sensor can record. Of course, higher megapixels can lead to larger image files and potentially more detail, but actual image quality also depends on factors like sensor size, optics, and compression. The other terms belong to different domains: MPEG is a video compression standard, MP3 is an audio compression format, and a multiplexer is a device that combines multiple signals into one.

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://bctmh.examzify.com

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