

CIPP-US^{Q&As}

Certified Information Privacy Professional/United States (CIPP/US)

Pass IAPP CIPP-US Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/cipp-us.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1**SCENARIO**

Please use the following to answer the next question:

You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider,

CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with

CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering

the contract, and has not conducted audits of CloudHealth's security measures.

A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been

published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals ?ones that exposed the PHI of public figures including celebrities and politicians.

During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law

enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.

A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted

a discovery request for the ePHI exposed in the breach.

Of the safeguards required by the HIPAA Security Rule, which of the following is NOT at issue due to HealthCo's actions?

- A. Administrative Safeguards
- B. Technical Safeguards
- C. Physical Safeguards
- D. Security Safeguards

Correct Answer: C

C: Administrative covers the phishing training. Technical covers the lack of encryption. Security safeguards are what we're talking about..and administrative and technical are important as mentioned above. The Physical safeguards are

not important to how this breach occurred.

QUESTION 2

Which of the following became the first state to pass a law specifically regulating the collection of biometric data?

- A. California.
- B. Texas.
- C. Illinois.
- D. Washington.

Correct Answer: C

Reference: <https://www.jdsupra.com/legalnews/state-biometric-laws-are-trending-and-2640319/>

QUESTION 3

What privacy concept grants a consumer the right to view and correct errors on his or her credit report?

- A. Access.
- B. Notice.
- C. Action.
- D. Choice.

Correct Answer: B

QUESTION 4

SCENARIO

Please use the following to answer the next question:

Miraculous Healthcare is a large medical practice with multiple locations in California and Nevada. Miraculous normally treats patients in person, but has recently decided to start offering telehealth appointments, where patients can have virtual appointments with on-site doctors via a phone app.

For this new initiative, Miraculous is considering a product built by MedApps, a company that makes quality telehealth apps for healthcare practices and licenses them to be used with the practices' branding. MedApps provides technical support for the app, which it hosts in the cloud. MedApps also offers an optional benchmarking service for providers who wish to compare their practice to others using the service.

Riya is the Privacy Officer at Miraculous, responsible for the practice's compliance with HIPAA and other applicable laws, and she works with the Miraculous procurement team to get vendor agreements in place. She occasionally

assists

procurement in vetting vendors and inquiring about their own compliance practices, as well as negotiating the terms of vendor agreements. Riya is currently reviewing the suitability of the MedApps app from a privacy perspective.

Riya has also been asked by the Miraculous Healthcare business operations team to review the MedApps' optional benchmarking service. Of particular concern is the requirement that Miraculous Healthcare upload information about the

appointments to a portal hosted by MedApps.

What HIPAA compliance issue would Miraculous have to consider before using the telehealth app?

- A. HIPAA does not permit healthcare providers to use cloud hosting services.
- B. HIPAA does not permit in-person appointment data to be hosted in the cloud.
- C. HIPAA would require Miraculous and MedApps to enter into a Business Associate Agreement.
- D. HIPAA would require Miraculous to obtain patient consent before in-person appointment data can be shared with third parties.

Correct Answer: D

Reference: <https://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html>

QUESTION 5

Which of the following is a U.S. surveillance program authorized under Section 702 of the Foreign Intelligence Surveillance Act Amendments Act?

- A. Upstream
- B. NATGRID
- C. Project 6
- D. SORM

Correct Answer: A

Reference: <https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf>

[CIPP-US Practice Test](#)

[CIPP-US Exam Questions](#)

[CIPP-US Braindumps](#)