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

California\\'s SB 1386 was the first law of its type in the United States to do what?

A. Require commercial entities to disclose a security data breach concerning personal information about the state\\'s residents

B. Require notification of non-California residents of a breach that occurred in California

C. Require encryption of sensitive information stored on servers that are Internet connected

D. Require state attorney general enforcement of federal regulations against unfair and deceptive trade practices

Correct Answer: A

Reference: https://corporate.findlaw.com/law-library/california-raises-the-bar-on-data-security-and-privacy.html

QUESTION 2

In March 2012, the FTC released a privacy report that outlined three core principles for companies handling consumer data. Which was NOT one of these principles?

A. Simplifying consumer choice.

B. Enhancing security measures.

C. Practicing Privacy by Design.

D. Providing greater transparency.

Correct Answer: B

Reference: https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

QUESTION 3

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.

Which of the following would be HealthCo\\'s best response to the attorney\\'s discovery request?

A. Reject the request because the HIPAA privacy rule only permits disclosure for payment, treatment or healthcare operations

B. Respond with a request for satisfactory assurances such as a qualified protective order

C. Turn over all of the compromised patient records to the plaintiff\\'s attorney

D. Respond with a redacted document only relative to the plaintiff

Correct Answer: C

QUESTION 4

Which is an exception to the general prohibitions on telephone monitoring that exist under the U.S. Wiretap Act?

A. Call center exception

B. Inter-company communications exception

C. Ordinary course of business exception

D. Internet calls exception

Correct Answer: C

Reference: https://www.lexology.com/library/detail.aspx?g=1031d6a6-19f5-4422-b5a2-98d7038905e9

QUESTION 5

SCENARIO

Please use the following to answer the next question:

You are the privacy manager at a privately-owned U.S. company that produces an increasingly popular tness app called GetFit. After users create an account with their contact information, the app uses a smartphone and a system of connected smartwatch sensors to track users when they exercise. It collects information on location when users walk or run outdoors, as well as general health information (such as heart rate) during all exercise sessions. The app also collects credit card information for payment of the monthly subscription fee.

One Friday, the company\\'s security team contacts you about the discovery of malware on their media server. The team assures you that there was no user data on this server and that, in any case, they found the malware before any damage could be done.

However, on Monday morning the security team contacts you again, this time with the information that they have discovered the same malware on the company\\'s payments server. They suspect it likely that users\\' credit card information was taken by the attacker. By Monday evening, the situation has gotten dramatically worse, as the security team has also discovered this malware on the company\\'s database server, an in ltration that gives the attacker access to users\\' pro le, health and location information.

After coordinating with the security team, you are asked to meet with senior management and advise them on the company\\'s obligations in connection with the incident. The Chief Financial O cer asks, "If we decide to notify all our users of this incident, are we obligated to provide any of them with a free credit monitoring offer?" The General Counsel wants to know if providing this notice and offer will help the company avoid liability.

Who, if anyone, would the company have to notify immediately following the security team\\'s rst call to the privacy manager on Friday?

A. It would have to notify each state\\'s attorney general\\'s o ce since the app is marketed to consumers.

B. It would not have to notify anyone since malware intrusions do not trigger breach noti cation laws.

C. It would have to notify the Federal Trade Commission (FTC) since there was an incident involving a mobile app.

D. It would not have to notify anyone since there was no unauthorized access of user data that would be considered personal information under applicable state laws.

Correct Answer: B