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.passapply.com/cipp-us.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What consumer protection did the Fair and Accurate Credit Transactions Act (FACTA) require?

A. The ability for the consumer to correct inaccurate credit report information

B. The truncation of account numbers on credit card receipts

C. The right to request removal from e-mail lists

D. Consumer notice when third-party data is used to make an adverse decision

Correct Answer: A

Reference: https://www.investopedia.com/terms/f/facta.asp

QUESTION 2

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.

What is the most effective kind of training CloudHealth could have given its employees to help prevent this type of data breach?

A. Training on techniques for identifying phishing attempts

B. Training on the terms of the contractual agreement with HealthCo

C. Training on the difference between confidential and non-public information

D. Training on CloudHealth\\'s HR policy regarding the role of employees involved data breaches

Correct Answer: A

QUESTION 3

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.

How does the Monday evening discovery of the malware on the company\\'s database server alter the company\\'s noti cation obligations, if at all?

A. This discovery requires notice also be provided to the U.S. Dept. of Health and Human Services since the impacted information includes health information.

B. This discovery has no effect on the situation, since the user information does not include a social security number or driver\\'s license number.

C. This discovery requires notice also be provided to the FTC since a health app is subject to the Health Breach Noti cation Rule.

D. This discovery has no effect on the situation, since all required noti cations are already being provided.

Correct Answer: C

QUESTION 4

Which of the following practices is NOT a key component of a data ethics framework?

A. Automated decision-making.

B. Preferability testing.

C. Data governance.

D. Auditing.

Correct Answer: A

QUESTION 5

Which of the following is NOT a principle found in the APEC Privacy Framework?

A. Integrity of Personal Information.

B. Access and Correction.

C. Preventing Harm.

D. Privacy by Design.

Correct Answer: D

Reference: https://www.google.com/url?sa=tandrct=jandq=andesrc=sandsource=webandcd=andved=2ahUKEwiqtJX4tPHvAhUQG-wKHUoGBgkQFjAHegQIBRADandurl=https%3A%2F%2Fwww.apec.org%2F-%2Fmedia%2FAPEC%2FPublications%2F2016%2F11%2F2016-CTI-Report-to-Ministers%2FTOC%2FAppendix-17-Updates-to-the-APEC-Privacy-Framework.pdfandusg=AOvVaw1Yysi4Ym_1VaCw1VZiB70a