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

In 2011, the FTC announced a settlement with Google regarding its social networking service Google Buzz. The FTC alleged that in the process of launching the service, the company did all of the following EXCEPT?

A. Violated its own privacy policies.

B. Engaged in deceptive trade practices.

C. Failed to comply with Safe Harbor principles.

D. Failed to employ sufficient security safeguards.

Correct Answer: D

Reference: https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz

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

Chanel Hair Studio is a busy high-end hair salon. In an effort to maximize efficiency of its operations and reduce wait times for appointments, Chanel decides to implement artificial intelligence software that will use client profiles and history to predict which clients will likely be late for their appointments. Information used to create the client profile included appointment history, distance from the salon, and any references to being tardy pulled from the client\\'s social media accounts. If a client is predicted to be late, their appointment will be cancelled within 5 minutes.

Based on the details, what is the biggest potential privacy concern related to Chanel\\'s use of this new software?

A. Scanning a client\\'s social media accounts to use in a client profile without notice to the client.

B. Calculating client profile address distance from the salon to determine location from salon to help predict if the client will be late.

C. Using client profile information for any purpose other than setting up an appointment.

D. Assessing client tardiness history with the salon for predictive purposes.

Correct Answer: B

QUESTION 4

SCENARIO

Please use the following to answer the next question:

Jane is a U.S. citizen and a senior software engineer at California-based Jones Labs, a major software supplier to the U.S. Department of Defense and other U.S. federal agencies. Jane\\'s manager, Patrick, is a French citizen who has been living in California for over a decade. Patrick has recently begun to suspect that Jane is an insider secretly transmitting trade secrets to foreign intelligence. Unbeknownst to Patrick, the FBI has already received a hint from anonymous whistleblower, and jointly with the National Security Agency is investigating Jane\\'s possible implication in a sophisticated foreign espionage campaign.

Ever since the pandemic, Jane has been working from home. To complete her daily tasks she uses her corporate

laptop, which after each login conspicuously provides notice that the equipment belongs to Jones Labs and may be monitored according to the enacted privacy policy and employment handbook. Jane also has a corporate mobile phone that she uses strictly for business, the terms of which are de ned in her employment contract and elaborated upon in her employee handbook. Both the privacy policy and the employee handbook are revised annually by a reputable California law rm specializing in privacy law. Jane also has a personal iPhone that she uses for private purposes only.

Jones Labs has its primary data center in San Francisco, which is managed internally by Jones Labs engineers. The secondary data center, managed by Amazon AWS, is physically located in the UK for disaster recovery purposes. Jones Labs\\' mobile devices backup is managed by a mid-sized mobile defense company located in Denver, which physically stores the data in Canada to reduce costs. Jones Labs MS O ce documents are securely stored in a Microsoft O ce 365 data center based in Ireland. Manufacturing data of Jones Labs is stored in Taiwan and managed by a local supplier that has no presence in the U.S.

Before inspecting any GPS geolocation data from Jane\\'s corporate mobile phone, Patrick should rst do what?

A. Obtain prior consent from Jane pursuant to the Telephone Consumer Protection Act

B. Revise emerging workplace privacy best practices with a reputable advocacy organization.

C. Obtain a subpoena from law enforcement, or a court order, directing Jones Labs to collect the GPS geolocation data.

D. Ensure that such activity is permitted under Jane\\'s employment contract or the company\\'s employee privacy policy.

Correct Answer: C

QUESTION 5

Which of the following is NOT one of three broad categories of products offered by data brokers, as identified by the U.S. Federal Trade Commission (FTC)?

A. Research (such as information for understanding consumer trends).

B. Risk mitigation (such as information that may reduce the risk of fraud).

C. Location of individuals (such as identifying an individual from partial information).

D. Marketing (such as appending data to customer information that a marketing company already has).

Correct Answer: C

Reference: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf