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

- **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:

A US-based startup company is selling a new gaming application. One day, the CEO of the company receives an urgent letter from a prominent EU-based retail partner. Triggered by an unresolved complaint lodged by an EU resident, the

letter describes an ongoing investigation by a supervisory authority into the retailer\\'s data handling practices.

The complainant accuses the retailer of improperly disclosing her personal data, without consent, to parties in the United States. Further, the complainant accuses the EU-based retailer of failing to respond to her withdrawal of consent and

request for erasure of her personal data. Your organization, the US-based startup company, was never informed of this request for erasure by the EU-based retail partner. The supervisory authority investigating the complaint has threatened

the suspension of data flows if the parties involved do not cooperate with the investigation. The letter closes with an urgent request: "Please act immediately by identifying all personal data received from our company."

This is an important partnership. Company executives know that its biggest fans come from Western Europe; and this retailer is primarily responsible for the startup\\'s rapid market penetration.

As the Company\\'s data privacy leader, you are sensitive to the criticality of the relationship with the retailer.

Under the GDPR, the complainant\\'s request regarding her personal information is known as what?

A. Right of Access

B. Right of Removal

C. Right of Rectification

D. Right to Be Forgotten

Correct Answer: B

QUESTION 2

If an organization maintains data classified as high sensitivity in the same system as data classified as low sensitivity, which of the following is the most likely outcome?

A. The organization will still be in compliance with most sector-specific privacy and security laws.

B. The impact of an organizational data breach will be more severe than if the data had been segregated.

C. Temporary employees will be able to find the data necessary to fulfill their responsibilities.

D. The organization will be able to address legal discovery requests efficiently without producing more information than necessary.

Correct Answer: B

Answer: B "Holding all data in one system can increase the consequences of a single breach" Excerpt From: "IAPP_US_TB_US-Private-Sector-Privacy-3E_1.0." Apple Books.

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.

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 4

One of the most signi cant elements of Senate Bill No. 260 relating to Internet privacy is the introduction of what term into Nevada law?

A. Data Ethics.

B. Data Brokers.

C. Arti cial Intelligence.

D. Transfer Mechanism.

Correct Answer: B

QUESTION 5

A nancial services company install "bossware" software on its employees\\' remote computers to monitor performance. The software logs screenshots, mouse movements, and keystrokes to determine whether an employee is being productive. The software can also enable the computer webcams to record video footage.

Which of the following would best support an employee claim for an intrusion upon seclusion tort?

A. The webcam is enabled to record video any time the computer is turned on.

B. The company creates and saves a biometric template for each employee based upon keystroke dynamics.

C. The software automatically sends a noti cation to a supervisor any time the employee\\'s mouse is dormant for more than ve minutes.

D. The webcam records video of an employee using a company laptop to perform personal business while at a coffee shop during work hours.

Correct Answer: D