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

The Clarifying Lawful Overseas Use of Data (CLOUD) Act is primarily intended to do which of the following?

A. Codify a treaty with the EU that permits the cross-border transfer of personal information from the EU to the United States in compliance with the General Data Protection Regulation (GDPR).

B. Update the legal mechanisms through which federal law enforcement may obtain data that service providers maintain in a foreign country.

C. Establish baseline privacy obligations that U.S. companies must comply with for personal information, even if stored in a foreign country.

D. Prohibit foreign companies from using the personal information of U.S. citizens without their consent.

Correct Answer: B

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 significant reason that the U.S. Department of Health and Human Services (HHS) might impose a penalty on HealthCo?

A. Because HealthCo did not require CloudHealth to implement appropriate physical and administrative measures to safeguard the ePHI

B. Because HealthCo did not conduct due diligence to verify or monitor CloudHealth\\'s security measures

C. Because HIPAA requires the imposition of a fine if a data breach of this magnitude has occurred

D. Because CloudHealth violated its contract with HealthCo by not encrypting the ePHI

Correct Answer: B

QUESTION 3

What do the Civil Rights Act, Pregnancy Discrimination Act, Americans with Disabilities Act, Age Discrimination Act, and Equal Pay Act all have in common?

A. They require employers not to discriminate against certain classes when employees use personal information

B. They require that employers provide reasonable accommodations to certain classes of employees

C. They afford certain classes of employees\\' privacy protection by limiting inquiries concerning their personal information

D. They permit employers to use or disclose personal information specifically about employees who are members of certain classes

Correct Answer: A

QUESTION 4

What was unique about the action that the Federal Trade Commission took against B.J.\\'s Wholesale Club in 2005?

A. It made third-party audits a penalty for policy violations.

B. It was based on matters of fairness rather than deception.

C. It was the first substantial U.S.-EU Safe Harbor enforcement.

D. It made user consent mandatory after any revisions of policy.

Correct Answer: A

Reference: https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges

QUESTION 5

Which of the following most accurately describes the regulatory status of pandemic contact-tracing apps in the United States?

A. Contact tracing is covered exclusively under the Health Insurance Portability and Accountability Act (HIPAA).

B. Contact tracing is regulated by the U.S. Centers for Disease Control and Prevention (CDC).

C. Contact tracing is subject to a patchwork of federal and state privacy laws.

D. Contact tracing is not regulated in the United States.

Correct Answer: C

QUESTION 6

Mega Corp. is a U.S.-based business with employees in California, Virginia, and Colorado. Which of the following must Mega Corp. comply with in regard to its human resources data?

A. California Privacy Rights Act.

B. California Privacy Rights Act and Virginia Consumer Data Protection Act.

C. California Privacy Rights Act and Colorado Privacy Act.

D. California Privacy Rights Act, Virginia Consumer Data Protection Act, and Colorado Privacy Act.

Correct Answer: D

QUESTION 7

SCENARIO

Please use the following to answer the next question:

Cheryl is the sole owner of Fitness Coach, Inc., a medium-sized company that helps individuals realize their physical fitness goals through classes, individual instruction, and access to an extensive indoor gym. She has owned the company

for ten years and has always been concerned about protecting customers\\' privacy while maintaining the highest level of service. She is proud that she has built long-lasting customer relationships.

Although Cheryl and her staff have tried to make privacy protection a priority, the company has no formal privacy policy. So Cheryl hired Janice, a privacy professional, to help her develop one.

After an initial assessment, Janice created a first of a new policy. Cheryl read through the draft and was concerned

about the many changes the policy would bring throughout the company. For example, the draft policy stipulates that a

customer\\'s personal information can only be held for one year after paying for a service such as a session with personal trainer. It also promises that customer information will not be shared with third parties without the written consent of the

customer. The wording of these rules worries Cheryl since stored personal information often helps her company to serve her customers, even if there are long pauses between their visits. In addition, there are some third parties that provide

crucial services, such as aerobics instructors who teach classes on a contract basis. Having access to customer files and understanding the fitness levels of their students helps instructors to organize their classes.

Janice understood Cheryl\\'s concerns and was already formulating some ideas for revision. She tried to put Cheryl at ease by pointing out that customer data can still be kept, but that it should be classified according to levels of sensitivity.

However, Cheryl was skeptical. It seemed that classifying data and treating each type differently would cause undue difficulties in the company\\'s day-to-day operations. Cheryl wants one simple data storage and access system that any

employee can access if needed.

Even though the privacy policy was only a draft, she was beginning to see that changes within her company were going to be necessary. She told Janice that she would be more comfortable with implementing the new policy gradually over a

period of several months, one department at a time. She was also interested in a layered approach by creating documents listing applicable parts of the new policy for each department.

What is the main problem with Cheryl\\'s suggested method of communicating the new privacy policy?

A. The policy would not be considered valid if not communicated in full.

B. The policy might not be implemented consistency across departments.

C. Employees would not be comfortable with a policy that is put into action over time.

D. Employees might not understand how the documents relate to the policy as a whole.

Correct Answer: B

QUESTION 8

Which of the following would best provide a sufficient consumer disclosure under the Fair Credit Reporting Act (FCRA) prior to a consumer report being obtained for employment purposes?

A. A standalone notice document.

B. A notice provision in a mailed offer letter.

C. A notice provision in an electronic employment application.

D. A verbal notice provided with a conditional offer of employment.

Correct Answer: A

QUESTION 9

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

QUESTION 10

A large online bookseller decides to contract with a vendor to manage Personal Information (PI). What is the least important factor for the company to consider when selecting the vendor?

A. The vendor\\'s reputation

B. The vendor\\'s financial health

C. The vendor\\'s employee retention rates

D. The vendor\\'s employee training program

Correct Answer: B

QUESTION 11

Which law provides employee benefits, but often mandates the collection of medical information?

A. The Occupational Safety and Health Act.

B. The Americans with Disabilities Act.

C. The Employee Medical Security Act.

D. The Family and Medical Leave Act.

Correct Answer: B

Reference: https://www.dph.illinois.gov/covid19/community-guidance/workplace-health-and-safety-guidance/employee-employer-rights-and-safety

QUESTION 12

All of the following organizations are specified as covered entities under the Health Insurance Portability and Accountability Act (HIPAA) EXCEPT?

A. Healthcare information clearinghouses

B. Pharmaceutical companies

C. Healthcare providers

D. Health plans

Correct Answer: B

Reference: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

QUESTION 13

A California resident has created an account on your company\\'s online food delivery platform and placed several orders in the past month. Later she submits a data subject request to access her personal information under the California Privacy Rights Act.

Assuming that the CPRA is in force, which of the following data elements would your company NOT have to provide to the requester once her identity has been veri ed?

A. Inferences made about the individual for the company\\'s internal purposes.

B. The loyalty account number assigned through the individual\\'s use of the services.

C. The time stamp for the creation of the individual\\'s account in the platform\\'s database.

D. The email address submitted by the individual as part of the account registration process.

Correct Answer: A

QUESTION 14

Which of the following best describes an employer\\'s privacy-related responsibilities to an employee who has left the workplace?

A. An employer has a responsibility to maintain a former employee\\'s access to computer systems and company data needed to support claims against the company such as discrimination.

B. An employer has a responsibility to permanently delete or expunge all sensitive employment records to minimize privacy risks to both the employer and former employee.

C. An employer may consider any privacy-related responsibilities terminated, as the relationship between employer and employee is considered primarily contractual.

D. An employer has a responsibility to maintain the security and privacy of any sensitive employment records retained for a legitimate business purpose.

Correct Answer: B

QUESTION 15

SCENARIO

Please use the following to answer the next question:

Otto is preparing a report to his Board of Directors at Filtration Station, where he is responsible for the privacy program. Filtration Station is a U.S. company that sells filters and tubing products to pharmaceutical companies for research use.

The company is based in Seattle, Washington, with offices throughout the U.S. and Asia. It sells to business customers across both the U.S. and the Asia-Pacific region. Filtration Station participates in the Cross-Border Privacy Rules system

of the APEC Privacy Framework.

Unfortunately, Filtration Station suffered a data breach in the previous quarter. An unknown third party was able to gain access to Filtration Station\\'s network and was able to steal data relating to employees in the company\\'s Human

Resources database, which is hosted by a third-party cloud provider based in the U.S. The HR data is encrypted. Filtration Station also uses the third-party cloud provider to host its business marketing contact database. The marketing

database was not affected by the data breach. It appears that the data breach was caused when a system administrator at the cloud provider stored the encryption keys with the data itself.

The Board has asked Otto to provide information about the data breach and how updates on new developments in

privacy laws and regulations apply to Filtration Station. They are particularly concerned about staying up to date on the various U.S. state laws and regulations that have been in the news, especially the California Consumer Privacy Act (CCPA) and breach notification requirements.

The Board has asked Otto whether the company will need to comply with the new California Consumer Privacy Law (CCPA). What should Otto tell the Board?

A. That CCPA will apply to the company only after the California Attorney General determines that it will enforce the statute.

B. That the company is governed by CCPA, but does not need to take any additional steps because it follows CPBR.

C. That business contact information could be considered personal information governed by CCPA.

D. That CCPA only applies to companies based in California, which exempts the company from compliance.

Correct Answer: A