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.pass4itsure.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

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

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

Which federal agency plays a role in privacy policy, but does NOT have regulatory authority?

A. The Office of the Comptroller of the Currency.

B. The Federal Communications Commission.

C. The Department of Transportation.

D. The Department of Commerce.

Correct Answer: C

QUESTION 4

Your company, which sells its products in the United States and the European Union, is seeking to purchase cloud storage from a multinational cloud storage provider. The engineering team at your company wants to set up cloud data centers from the storage provider in both the United States and Germany.

Which of the following contractual provisions should be included in the contract to ensure the security of the personal data being stored in both data center locations?

A. An audit provision that allows the cloud storage provider to restrict an independent auditor\\'s access to the premises, documents and personnel involved in the cloud storage provider\\'s processing of the data.

B. A general authorization provision that allows the cloud storage provider to appoint subcontractors to help provide the cloud storage services.

C. A purpose limitation provision that requires the data, including personal information, to only be used for the contracted purposes.

D. A non-solicitation provision prohibiting both companies from seeking to hire employees of the other company.

Correct Answer: C

QUESTION 5

According to the FTC Report of 2012, what is the main goal of Privacy by Design?

A. Obtaining consumer consent when collecting sensitive data for certain purposes

B. Establishing a system of self-regulatory codes for mobile-related services

C. Incorporating privacy protections throughout the development process

D. Implementing a system of standardization for privacy notices

Correct Answer: C

Reference: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

QUESTION 6

Which of the following conditions would NOT be su cient to excuse an entity from providing breach noti cation under state law?

A. If the data involved was encrypted.

B. If the data involved was accessed but not exported.

C. If the entity was subject to the GLBA Safeguards Rule.

D. If the entity followed internal noti cation procedures compatible with state law.

Correct Answer: C

QUESTION 7

What information did the Red Flag Program Clarification Act of 2010 add to the original Red Flags rule?

A. The most common methods of identity theft.

B. The definition of what constitutes a creditor.

C. The process for proper disposal of sensitive data.

D. The components of an identity theft detection program.

Correct Answer: B

Reference: https://www.healthcareitnews.com/news/obama-makes-docs-exemption-red-flags-rule-law

QUESTION 8

SCENARIO

Please use the following to answer the next question:

Noah is trying to get a new job involving the management of money. He has a poor personal credit rating, but he has made better financial decisions in the past two years.

One potential employer, Arnie\\'s Emporium, recently called to tell Noah he did not get a position. As part of the application process, Noah signed a consent form allowing the employer to request his credit report from a consumer reporting

agency (CRA). Noah thinks that the report hurt his chances, but believes that he may not ever know whether it was his credit that cost him the job. However, Noah is somewhat relieved that he was not offered this particular position. He

noticed that the store where he interviewed was extremely disorganized. He imagines that his credit report could still

be sitting in the office, unsecured.

Two days ago, Noah got another interview for a position at Sam\\'s Market. The interviewer told Noah that his credit report would be a factor in the hiring decision. Noah was surprised because he had not seen anything on paper about this

when he applied.

Regardless, the effect of Noah\\'s credit on his employability troubles him, especially since he has tried so hard to improve it. Noah made his worst financial decisions fifteen years ago, and they led to bankruptcy. These were decisions he

made as a young man, and most of his debt at the time consisted of student loans, credit card debt, and a few unpaid bills ?all of which Noah is still working to pay off. He often laments that decisions he made fifteen years ago are still

affecting him today.

In addition, Noah feels that an experience investing with a large bank may have contributed to his financial troubles. In 2007, in an effort to earn money to help pay off his debt, Noah talked to a customer service representative at a large

investment company who urged him to purchase stocks. Without understanding the risks, Noah agreed. Unfortunately, Noah lost a great deal of money.

After losing the money, Noah was a customer of another financial institution that suffered a large security breach. Noah was one of millions of customers whose personal information was compromised. He wonders if he may have been a

victim of identity theft and whether this may have negatively affected his credit.

Noah hopes that he will soon be able to put these challenges behind him, build excellent credit, and find the perfect job.

Based on the scenario, which legislation should ease Noah\\'s worry about his credit report as a result of applying at Arnie\\'s Emporium?

A. The Privacy Rule under the Gramm-Leach-Bliley Act (GLBA).

B. The Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA).

C. The Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA).

D. The Red Flags Rule under the Fair and Accurate Credit Transactions Act (FACTA).

Correct Answer: B

QUESTION 9

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 10

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 11

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 12

What is an exception to the Electronic Communications Privacy Act of 1986 ban on interception of wire, oral and electronic communications?

A. Where one of the parties has given consent

B. Where state law permits such interception

C. If an organization intercepts an employee\\'s purely personal call

D. Only if all parties have given consent

Correct Answer: A

The prohibition on interception has a number of exceptions, each of which may have its own nuances requiring an expert to analyze. Under federal law, interception is permitted if a person is the party to the call or if one of the parties has given consent.69

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

What is the most likely reason that states have adopted their own data breach notification laws?

A. Many states have unique types of businesses that require specific legislation

B. Many lawmakers believe that federal enforcement of current laws has not been effective

C. Many types of organizations are not currently subject to federal laws regarding breaches

D. Many large businesses have intentionally breached the personal information of their customers

Correct Answer: B

QUESTION 15

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

Latest CIPP-US Dumps CIPP-US PDF Dumps CIPP-US Braindumps