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.pass2lead.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:

When there was a data breach involving customer personal and financial information at a large retail store, the company\\'s directors were shocked. However, Roberta, a privacy analyst at the company and a victim of identity theft herself, was

not. Prior to the breach, she had been working on a privacy program report for the executives. How the company shared and handled data across its organization was a major concern. There were neither adequate rules about access to

customer information nor

procedures for purging and destroying outdated data. In her research, Roberta had discovered that even low-level employees had access to all of the company\\'s customer data, including financial records, and that the company still had in its

possession obsolete customer data going back to the 1980s.

Her report recommended three main reforms. First, permit access on an as-needs-to-know basis. This would mean restricting employees\\' access to customer information to data that was relevant to the work performed. Second, create a highly secure database for storing customers\\' financial information (e.g., credit card and bank account numbers) separate from less sensitive information. Third, identify outdated customer information and then develop a process for securely disposing of it.

When the breach occurred, the company\\'s executives called Roberta to a meeting where she presented the recommendations in her report. She explained that the company having a national customer base meant it would have to ensure that it complied with all relevant state breach notification laws. Thanks to Roberta\\'s guidance, the company was able to notify customers quickly and within the specific timeframes set by state breach notification laws.

Soon after, the executives approved the changes to the privacy program that Roberta recommended in her report. The privacy program is far more effective now because of these changes and, also, because privacy and security are now considered the responsibility of every employee.

What could the company have done differently prior to the breach to reduce their risk?

A. Implemented a comprehensive policy for accessing customer information.

B. Honored the promise of its privacy policy to acquire information by using an opt-in method.

C. Looked for any persistent threats to security that could compromise the company\\'s network.

D. Communicated requests for changes to users\\' preferences across the organization and with third parties.

Correct Answer: C

QUESTION 2

U.S.

federal laws protect individuals from employment discrimination based on all of the following EXCEPT?

A.

Age.

B.

Pregnancy.

C.

Marital status.

D.

Genetic information.

Correct Answer: B

QUESTION 3

Which of the following describes the most likely risk for a company developing a privacy policy with standards that are much higher than its competitors?

A. Being more closely scrutinized for any breaches of policy

B. Getting accused of discriminatory practices

C. Attracting skepticism from auditors

D. Having a security system failure

Correct Answer: A

QUESTION 4

Privacy Is Hiring Inc., a CA-based company, is an online specialty recruiting firm focusing on placing privacy professionals in roles at major companies. Job candidates create online profiles outlining their experience and credentials, and can pay $19.99/month via credit card to have their profiles promoted to potential employers. Privacy Is Hiring Inc. keeps all customer data at rest encrypted on its servers.

Under what circumstances would Privacy Is Hiring Inc., need to notify affected individuals in the event of a data breach?

A. If law enforcement has completed its investigation and has authorized Privacy Is Hiring Inc. to provide the notification to clients and applicable regulators.

B. If the job candidates\\' credit card information and the encryption keys were among the information taken.

C. If Privacy Is Hiring Inc., reasonably believes that job candidates will be harmed by the data breach.

D. If the personal information stolen included the individuals\\' names and credit card pin numbers.

Correct Answer: D

QUESTION 5

A covered entity suffers a ransomware attack that affects the personal health information (PHI) of more than 500 individuals. According to Federal law under HIPAA, which of the following would the covered entity NOT have to report the breach to?

A. Department of Health and Human Services

B. The affected individuals

C. The local media

D. Medical providers

Correct Answer: D

Reference: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (page 6)

QUESTION 6

Which of the following best describes the ASIA-Pacific Economic Cooperation (APEC) principles?

A. A bill of rights for individuals seeking access to their personal information.

B. A code of responsibilities for medical establishments to uphold privacy laws.

C. An international court ruling on personal information held in the commercial sector.

D. A baseline of marketers\\' minimum responsibilities for providing opt-out mechanisms.

Correct Answer: A

Reference: http://documents1.worldbank.org/curated/en/751621525705087132/text/WPS8431.txt

QUESTION 7

The U.S. Supreme Court has recognized an individual\\'s right to privacy over personal issues, such as contraception, by acknowledging which of the following?

A. Federal preemption of state constitutions that expressly recognize an individual right to privacy.

B. A "penumbra" of unenumerated constitutional rights as well as more general protections of due process of law.

C. An interpretation of the U.S. Constitution\\'s explicit definition of privacy that extends to personal issues.

D. The doctrine of stare decisis, which allows the U.S. Supreme Court to follow the precedent of previously decided case law.

Correct Answer: B

Reference: https://academic.oup.com/idpl/article/2/4/255/676934

QUESTION 8

Your company\\'s most brilliant engineer develops a new Artificial Intelligence (AI) technology he calls OXO-2576. The engineer wants to begin using it to analyze all of the data your company collects about its customers. As the company\\'s privacy professional, you have some privacy concerns about using AI technology with customer data.

Which of the following is the best recommendation to offer the company?

A. Do not publicize that the company is using AI technology with its customer data.

B. De-identify the data collected by the AI technology so it cannot be linked to any individuals.

C. Automate the AI technology so there is no human seeing or handling the customers\\' personal information.

D. Use the AI technology only for employees, as companies are given more leeway when handling employee personal information.

Correct Answer: B

QUESTION 9

Which is an exception to the general prohibitions on telephone monitoring that exist under the U.S. Wiretap Act?

A. Call center exception

B. Inter-company communications exception

C. Ordinary course of business exception

D. Internet calls exception

Correct Answer: C

Reference: https://www.lexology.com/library/detail.aspx?g=1031d6a6-19f5-4422-b5a2-98d7038905e9

QUESTION 10

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 11

Sarah lives in San Francisco, California. Based on a dramatic increase in unsolicited commercial emails, Sarah believes that a major social media platform with over 50 million users has collected a lot of personal information about her. The company that runs the platform is based in New York and France.

Why is Sarah entitled to ask the social media platform to delete the personal information they have collected about her?

A. Any company with a presence in Europe must comply with the General Data Protection Regulation globally, including in response to data subject deletion requests.

B. Under Section 5 of the FTC Act, the Federal Trade Commission has held that refusing to delete an individual\\'s personal information upon request constitutes an unfair practice.

C. The California Consumer Privacy Act entitles Sarah to request deletion of her personal information.

D. The New York "Stop Hacks and Improve Electronic Data Security" (SHIELD) Act requires that businesses under New York\\'s jurisdiction must delete customers\\' personal information upon request.

Correct Answer: C

Reference: https://www.varonis.com/blog/ccpa-vs-gdpr/

QUESTION 12

Which of the following is most likely to provide privacy protection to private-sector employees in the United States?

A. State law, contract law, and tort law

B. The Federal Trade Commission Act (FTC Act)

C. Amendments one, four, and five of the U.S. Constitution

D. The U.S. Department of Health and Human Services (HHS)

Correct Answer: A

Reference: https://corporate.findlaw.com/law-library/right-to-privacy-in-the-workplace-in-the-information-age.html

QUESTION 13

SCENARIO

Please use the following to answer the next question:

Matt went into his son\\'s bedroom one evening and found him stretched out on his bed typing on his laptop.

"Doing your homework?" Matt asked hopefully.

"No," the boy said. "I\\'m filling out a survey."

Matt looked over his son\\'s shoulder at his computer screen. "What kind of survey?"

"It\\'s asking questions about my opinions."

"Let me see," Matt said, and began reading the list of questions that his son had already answered. "It\\'s asking your opinions about the government and citizenship. That\\'s a little odd. You\\'re only ten."

Matt wondered how the web link to the survey had ended up in his son\\'s email inbox. Thinking the message might have been sent to his son by mistake he opened it and read it. It had come from an entity called the Leadership Project, and

the content and the graphics indicated that it was intended for children. As Matt read further he learned that kids who took the survey were automatically registered in a contest to win the first book in a series about famous leaders.

To Matt, this clearly seemed like a marketing ploy to solicit goods and services to children. He asked his son if he had been prompted to give information about himself in order to take the survey. His son told him he had been asked to give his

name, address, telephone number, and date of birth, and to answer questions about his favorite games and toys.

Matt was concerned. He doubted if it was legal for the marketer to collect information from his son in the way that it was. Then he noticed several other commercial emails from marketers advertising products for children in his son\\'s inbox, and

he decided it was time to report the incident to the proper authorities.

Depending on where Matt lives, the marketer could be prosecuted for violating which of the following?

A. Investigative Consumer Reporting Agencies Act.

B. Unfair and Deceptive Acts and Practices laws.

C. Consumer Bill of Rights.

D. Red Flag Rules.

Correct Answer: B

QUESTION 14

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 15

Read this notice:

Our website uses cookies. Cookies allow us to identify the computer or device you\\'re using to access the site, but they don\\'t identify you personally. For instructions on setting your Web browser to refuse cookies, click here.

What type of legal choice does not notice provide?

A. Mandatory

B. Implied consent

C. Opt-in

D. Opt-out

Correct Answer: B