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:

Felicia has spent much of her adult life overseas, and has just recently returned to the U.S. to help her friend Celeste open a jewelry store in California. Felicia, despite being excited at the prospect, has a number of security concerns, and has

only grudgingly accepted the need to hire other employees. In order to guard against the loss of valuable merchandise, Felicia wants to carefully screen applicants. With their permission, Felicia would like to run credit checks, administer

polygraph tests, and scrutinize videos of interviews. She intends to read applicants\\' postings on social media, ask questions about drug addiction, and solicit character references. Felicia believes that if potential employees are serious about

becoming part of a dynamic new business, they will readily agree to these requirements.

Felicia is also in favor of strict employee oversight. In addition to protecting the inventory, she wants to prevent mistakes during transactions, which will require video monitoring. She also wants to regularly check the company vehicle\\'s GPS

for locations visited by employees. She also believes that employees who use their own devices for work-related purposes should agree to a certain amount of supervision.

Given her high standards, Felicia is skeptical about the proposed location of the store. She has been told that many types of background checks are not allowed under California law. Her friend Celeste thinks these worries are unfounded, as

long as applicants verbally agree to the checks and are offered access to the results. Nor does Celeste share Felicia\\'s concern about state breach notification laws, which, she claims, would be costly to implement even on a minor scale.

Celeste believes that

even if the business grows a customer database of a few thousand, it\\'s unlikely that a state agency would hassle an honest business if an accidental security incident were to occur.

In any case, Celeste feels that all they need is common sense ?like remembering to tear up sensitive documents before throwing them in the recycling bin. Felicia hopes that she\\'s right, and that all of her concerns will be put to rest next

month when their new business consultant (who is also a privacy professional) arrives from North Carolina.

Which law will be most relevant to Felicia\\'s plan to ask applicants about drug addiction?

A. The Americans with Disabilities Act (ADA).

B. The Occupational Safety and Health Act (OSHA).

C. The Genetic Information Nondiscrimination Act of 2008.

D. The Health Insurance Portability and Accountability Act (HIPAA).

Correct Answer: A

Reference: https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/personswithaddictions.aspx

QUESTION 2

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.

What answer should be given to the General Counsel?

A. "Users can only sue us if we violate the state breach noti cation laws."

B. "This is a health data incident subject to HIPAA, so the private right of action does not apply."

C. "Users cannot sue us, because only federal and state regulators have enforcement authority in data breaches."

D. "Even if we provide notice, we may still face liability due to mishandling the data and causing potential harm to users."

Correct Answer: D

QUESTION 3

SCENARIO

Please use the following to answer the next question:

Miraculous Healthcare is a large medical practice with multiple locations in California and Nevada. Miraculous normally treats patients in person, but has recently decided to start offering telehealth appointments, where patients can have

virtual appointments with on-site doctors via a phone app.

For this new initiative, Miraculous is considering a product built by MedApps, a company that makes quality telehealth apps for healthcare practices and licenses them to be used with the practices' branding. MedApps provides technical

support for the app, which it hosts in the cloud. MedApps also offers an optional benchmarking service for providers who wish to compare their practice to others using the service.

Riya is the Privacy Officer at Miraculous, responsible for the practice\\'s compliance with HIPAA and other applicable laws, and she works with the Miraculous procurement team to get vendor agreements in place. She occasionally assists

procurement in vetting vendors and inquiring about their own compliance practices, as well as negotiating the terms of vendor agreements. Riya is currently reviewing the suitability of the MedApps app from a privacy perspective.

Riya has also been asked by the Miraculous Healthcare business operations team to review the MedApps' optional benchmarking service. Of particular concern is the requirement that Miraculous Healthcare upload information about the appointments to a portal hosted by MedApps.

Which of the following would accurately describe the relationship of the parties if they enter into a contract for use of the app?

A. Miraculous Healthcare would be the covered entity because its name and branding are on the app; MedApps would be a business associate because it is hosting the data that supports the app.

B. MedApps would be the covered entity because it built and hosts the app and all the data; Miraculous Healthcare would be a business associate because it only provides its brand on the app.

C. Miraculous Healthcare would be a covered entity because it is the healthcare provider; MedApps would also be a covered entity because the data in the app is being shared with it.

D. Miraculous Healthcare would be the covered entity because it is the healthcare provider; MedApps would be a business associate because it is providing a service to support Miraculous.

Correct Answer: D

Reference: https://www.truevault.com/resources/compliance/what-is-a-covered-entity#:~:text=A%20covered%20entity%20is%20anyone,Covered%20Entities%20Include%3Aandtext=Nursing%20home%2C%20pharmacy%2C%20hospital%20or,programs%20that%20pay%20for%20healthcare

QUESTION 4

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 5

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