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

Which of the following statements is most accurate in regard to data breach notifications under federal and state laws:

A. You must notify the Federal Trade Commission (FTC) in addition to affected individuals if over 500 individuals are receiving notice.

B. When providing an individual with required notice of a data breach, you must identify what personal information was actually or likely compromised.

C. When you are required to provide an individual with notice of a data breach under any state\\'s law, you must provide the individual with an offer for free credit monitoring.

D. The only obligations to provide data breach notification are under state law because currently there is no federal law or regulation requiring notice for the breach of personal information.

Correct Answer: B

Reference: https://www.itgovernanceusa.com/data-breach-notification-laws

QUESTION 2

SCENARIO

Please use the following to answer the next question:

Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state\\'s Do Not Call list, as well as the people on it. "If they

were really serious about not being bothered," Evan said, "They\\'d be on the national DNC list. That\\'s the only one we\\'re required to follow. At SunriseLynx, we call until they ask us not to."

Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call "another time." This, to Larry, is a clear indication that they don\\'t want to be called at all. Evan doesn\\'t see it that way.

Larry believes that Evan\\'s arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly,

even connecting with employees on social media. However, following Evan\\'s political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.

Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common

at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan\\'s leadership.

Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations

sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned

this to a coworker, his concern was met with a shrug. It was the coworker\\'s belief that employees agreed to be monitored

when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an

outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.

Larry wants to take action, but is uncertain how to proceed.

In what area does Larry have a misconception about private-sector employee rights?

A. The applicability of federal law

B. The enforceability of local law

C. The strict nature of state law

D. The definition of tort law

Correct Answer: A

QUESTION 3

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 4

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 5

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.

Based on Felicia\\'s Bring Your Own Device (BYOD) plan, the business consultant will most likely advise Felicia and Celeste to do what?

A. Reconsider the plan in favor of a policy of dedicated work devices.

B. Adopt the same kind of monitoring policies used for work-issued devices.

C. Weigh any productivity benefits of the plan against the risk of privacy issues.

D. Make employment decisions based on those willing to consent to the plan in writing.

Correct Answer: D