

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.certbus.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

The FTC often negotiates consent decrees with companies found to be in violation of privacy principles. How does this benefit both parties involved?

- A. It standardizes the amount of fines.
- B. It simplifies the audit requirements.
- C. It avoids potentially harmful publicity.
- D. It spares the expense of going to trial.

Correct Answer: C

QUESTION 2

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

QUESTION 3

SCENARIO

Please use the following to answer the next question:

Declan has just started a job as a nursing assistant in a radiology department at Woodland Hospital. He has also started a program to become a registered nurse.

Before taking this career path, Declan was vaguely familiar with the Health Insurance Portability and Accountability Act (HIPAA). He now knows that he must help ensure the security of his patients' Protected Health Information (PHI).

Therefore, he is thinking carefully about privacy issues.

On the morning of his first day, Declan noticed that the newly hired receptionist handed each patient a HIPAA privacy notice. He wondered if it was necessary to give these privacy notices to returning patients, and if the radiology department

could reduce paper waste through a system of one-time distribution.

He was also curious about the hospital's use of a billing company. He questioned whether the hospital was doing all it could to protect the privacy of its patients if the billing company had details about patients' care.

On his first day Declan became familiar with all areas of the hospital's large radiology department. As he was organizing equipment left in the hallway, he overheard a conversation between two hospital administrators. He was surprised to

hear that a portable hard drive containing non-encrypted patient information was missing. The administrators expressed relief that the hospital would be able to avoid liability. Declan was surprised, and wondered whether the hospital had plans to properly report what had happened.

Despite Declan's concern about this issue, he was amazed by the hospital's effort to integrate Electronic Health Records (EHRs) into the everyday care of patients. He thought about the potential for streamlining care even more if they were accessible to all medical facilities nationwide.

Declan had many positive interactions with patients. At the end of his first day, he spoke to one patient, John, whose father had just been diagnosed with a degenerative muscular disease. John was about to get blood work done, and he feared that the blood work could reveal a genetic predisposition to the disease that could affect his ability to obtain insurance coverage. Declan told John that he did not think that was possible, but the patient was wheeled away before he could explain why. John plans to ask a colleague about this.

In one month, Declan has a paper due for one of his classes on a health topic of his choice. By then, he will have had many interactions with patients he can use as examples. He will be pleased to give credit to John by name for inspiring him to think more carefully about genetic testing.

Although Declan's day ended with many questions, he was pleased about his new position.

What is the most likely way that Declan might directly violate the Health Insurance Portability and Accountability Act (HIPAA)?

- A. By being present when patients are checking in
- B. By speaking to a patient without prior authorization
- C. By ignoring the conversation about a potential breach
- D. By following through with his plans for his upcoming paper

Correct Answer: D

"Other than for treatment, covered entities must make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary in order to accomplish the intended purpose." He isn't involved in the potential breach, which is why he isn't trained for it, and doesn't know all the facts of the situation. He has no obligation and doesn't need to investigate any further based on anything that he heard.

QUESTION 4

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 draft 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 a 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.

Based on the scenario, which of the following would have helped Janice to better meet the company's needs?

- A. Creating a more comprehensive plan for implementing a new policy
- B. Spending more time understanding the company's information goals
- C. Explaining the importance of transparency in implementing a new policy
- D. Removing the financial burden of the company's employee training program

Correct Answer: B

QUESTION 5

Which of the following conditions would NOT be sufficient to excuse an entity from providing breach notification 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 notification procedures compatible with state law.

Correct Answer: C

QUESTION 6

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 7

Which federal law or regulation preempts state law?

- A. Health Insurance Portability and Accountability Act
- B. Controlling the Assault of Non-Solicited Pornography and Marketing Act
- C. Telemarketing Sales Rule
- D. Electronic Communications Privacy Act of 1986

Correct Answer: B

QUESTION 8

If an organization certified under Privacy Shield wants to transfer personal data to a third party acting as an agent, the organization must ensure the third party does all of the following EXCEPT?

- A. Uses the transferred data for limited purposes
- B. Provides the same level of privacy protection as the organization
- C. Notifies the organization if it can no longer meet its requirements for proper data handling
- D. Enters a contract with the organization that states the third party will process data according to the consent agreement

Correct Answer: D

Reference: <https://www.privacyshield.gov/Key-New-Requirements>

QUESTION 9

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.

Which act would authorize Evan's undercover investigation?

- A. The Whistleblower Protection Act
- B. The Stored Communications Act (SCA)
- C. The National Labor Relations Act (NLRA)
- D. The Fair and Accurate Credit Transactions Act (FACTA)

Correct Answer: B

Stored communications. As previously discussed, the SCA creates a general prohibition against the unauthorized acquisition, alteration or blocking of electronic communications while in electronic storage in a facility through which an electronic communications service is provided.¹¹⁹ Violations for interceptions can lead to criminal penalties or a civil lawsuit. The law provides for exceptions. Two exceptions that may apply to the employer are for conduct authorized:

"By the person or entity providing a wire or electronic communications service" (often the employer)¹²⁰ "By a user of that service with respect to a communication of or intended for that user"¹²¹

QUESTION 10

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 11

Which of the following would NOT be considered a method of obtaining verifiable parental consent before collecting, using or disclosing personal information from children under the Children's Online Privacy Protection Act (COPPA) of 1998?

- A. Using a credit card, debit card, or other online payment system.
- B. Having the parent call a toll-free telephone number staffed by trained personnel.
- C. Having the parent sign a consent form and return it to the operator by postal mail, facsimile, or electronic scan.
- D. Sending a text message to the parent explaining the intended uses of the information.

Correct Answer: D

Reference: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#l.%20Verifiable%20Parental%20Consent>

QUESTION 12

Under the Telemarketing Sales Rule, what characteristics of consent must be in place for an organization to acquire an exception to the Do-Not-Call rules for a particular consumer?

- A. The consent must be in writing, must state the times when calls can be made to the consumer and must be signed
- B. The consent must be in writing, must contain the number to which calls can be made and must have an end date
- C. The consent must be in writing, must contain the number to which calls can be made and must be signed
- D. The consent must be in writing, must have an end date and must state the times when calls can be made

Correct Answer: C

C: "The TSR allows sellers and telemarketers to call consumers who consent to receive such calls. This consent must be in writing, must state the number to which calls may be made, and must include the consumer's signature. (A valid electronic signature is acceptable.)"

QUESTION 13

When does the Telemarketing Sales Rule require an entity to share a do-not-call request across its organization?

- A. When the operational structures of its divisions are not transparent
- B. When the goods and services sold by its divisions are very similar

- C. When a call is not the result of an error or other unforeseen cause
- D. When the entity manages user preferences through multiple platforms

Correct Answer: C

QUESTION 14

A financial services company install "bossware" software on its employees' remote computers to monitor performance. The software logs screenshots, mouse movements, and keystrokes to determine whether an employee is being productive. The software can also enable the computer webcams to record video footage.

Which of the following would best support an employee claim for an intrusion upon seclusion tort?

- A. The webcam is enabled to record video any time the computer is turned on.
- B. The company creates and saves a biometric template for each employee based upon keystroke dynamics.
- C. The software automatically sends a notification to a supervisor any time the employee's mouse is dormant for more than five minutes.
- D. The webcam records video of an employee using a company laptop to perform personal business while at a coffee shop during work hours.

Correct Answer: D

QUESTION 15

What are banks required to do under the Gramm-Leach-Bliley Act (GLBA)?

- A. Conduct annual consumer surveys regarding satisfaction with user preferences
- B. Process requests for changes to user preferences within a designated time frame
- C. Provide consumers with the opportunity to opt out of receiving telemarketing phone calls
- D. Offer an Opt-Out before transferring PI to an unaffiliated third party for the latter's own use

Correct Answer: D

Reference: <https://www.investopedia.com/terms/g/glba.asp>

[CIPP-US VCE Dumps](#)

[CIPP-US Study Guide](#)

[CIPP-US Braindumps](#)