

# QUESTIONS & ANSWERS

Kill your exam at first Attempt



CIPP-US Dumps  
CIPP-US Braindumps  
CIPP-US Real Questions  
CIPP-US Practice Test  
CIPP-US dumps free



**IAPP**

# CIPP-US

*Certified Information Privacy Professional/United States (CIPP/US)*

<http://killexams.com/pass4sure/exam-detail/CIPP-US>



**Question: 75**

Within what time period must a commercial message sender remove a recipient's address once they have asked to stop receiving future e-mail?

- A . 7 days
- B . 10 days
- C . 15 days
- D . 21 days

**Answer: B**

Explanation:

Reference: <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>

**Question: 76**

**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 regard to telemarketing practices, Evan the supervisor has a misconception regarding?

- A . The conditions under which recipients can opt out
- B . The wishes of recipients who request callbacks
- C . The right to monitor calls for quality assurance
- D . The relationship of state law to federal law

**Answer: B**

**Question: 77**

Which of the following federal agencies does NOT enforce the Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA)?

- A . The Office of the Comptroller of the Currency
- B . The Consumer Financial Protection Bureau
- C . The Department of Health and Human Services
- D . The Federal Trade Commission

**Answer: C**

Explanation:

Reference: [https://en.wikipedia.org/wiki/Fair\\_and\\_Accurate\\_Credit\\_Transactions\\_Act](https://en.wikipedia.org/wiki/Fair_and_Accurate_Credit_Transactions_Act)

**Question: 78**

Which entities must comply with the Telemarketing Sales Rule?

- A . For-profit organizations and for-profit telefundraisers regarding charitable solicitations
- B . Nonprofit organizations calling on their own behalf
- C . For-profit organizations calling businesses when a binding contract exists between them
- D . For-profit and not-for-profit organizations when selling additional services to establish customers

**Answer: D**

Explanation:

Reference: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule>

**Question: 79**

In 2014, Google was alleged to have violated the Family Educational Rights and Privacy Act (FERPA) through its Apps for Education suite of tools.

For what specific practice did students sue the company?

- A . Scanning emails sent to and received by students
- B . Making student education records publicly available
- C . Relying on verbal consent for a disclosure of education records
- D . Disclosing education records without obtaining required consent

**Answer: A**

Explanation:

Reference: <https://www.edweek.org/ew/articles/2014/03/13/26google.h33.html>

**Question: 80**

Most states with data breach notification laws indicate that notice to affected individuals must be sent in the “most expeditious time possible without unreasonable delay.”

By contrast, which of the following states currently imposes a definite limit for notification to affected individuals?

- A . Maine
- B . Florida
- C . New York
- D . California

**Answer: B**

Explanation:

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

**Question: 81**

In what way does the “Red Flags Rule” under the Fair and Accurate Credit Transactions Act (FACTA) relate to the owner of a grocery store who uses a money wire service?

- A . It mandates the use of updated technology for securing credit records
- B . It requires the owner to implement an identity theft warning system
- C . It is not usually enforced in the case of a small financial institution
- D . It does not apply because the owner is not a creditor

**Answer: A**

**Question: 82**

What was the original purpose of the Federal Trade Commission Act?

- A . To ensure privacy rights of
- C . citizens
- D . To protect consumers
- E . To enforce antitrust laws
- F . To negotiate consent decrees with companies violating personal privacy

**Answer: B**

Explanation:

Reference: <https://www.ftc.gov/about-ftc>

**Question: 83**

**SCENARIO**

Please use the following to answer the next QUESTION:

A US-based startup company is selling a new gaming application. One day, the CEO of the company receives an urgent letter from a prominent EU-based retail partner. Triggered by an unresolved complaint lodged by an EU resident, the letter describes an ongoing investigation by a supervisory authority into the retailer's data handling practices.

The complainant accuses the retailer of improperly disclosing her personal data, without consent, to parties in the United States. Further, the complainant accuses the EU-based retailer of failing to respond to her withdrawal of consent and request for erasure of her personal data. Your organization, the US-based startup company, was never informed of this request for erasure by the EU-based retail partner. The supervisory authority investigating the complaint has threatened the suspension of data flows if the parties involved do not cooperate with the investigation. The letter closes with an urgent request: "Please act immediately by identifying all personal data received from our company."

This is an important partnership. Company executives know that its biggest fans come from Western Europe; and this retailer is primarily responsible for the startup's rapid market penetration.

As the Company's data privacy leader, you are sensitive to the criticality of the relationship with the retailer.

Upon review, the data privacy leader discovers that the Company's documented data inventory is obsolete.

What is the data privacy leader's next best source of information to aid the investigation?

- A . Reports on recent purchase histories
- B . Database schemas held by the retailer
- C . Lists of all customers, sorted by country
- D . Interviews with key marketing personnel

**Answer: C**

**Question: 84**

**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 C 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 significant reason that the U.S. Department of Health and Human Services (HHS) might impose a penalty on HealthCo?

- A. Because HealthCo did not require CloudHealth to implement appropriate physical and administrative measures to safeguard the ePHI
- B. Because HealthCo did not conduct due diligence to verify or monitor CloudHealth's security measures
- C. Because HIPAA requires the imposition of a fine if a data breach of this magnitude has occurred
- D. Because CloudHealth violated its contract with HealthCo by not encrypting the ePHI

**Answer: B**

**Question: 85**

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.

**Answer:** B

For More exams visit <https://killexams.com/vendors-exam-list>



*Kill your exam at First Attempt....Guaranteed!*