

100% Pass Quiz IAPP - High Pass-Rate CIPP-US - Pass Certified Information Privacy Professional/United States (CIPP/US) Test



P.S. Free & New CIPP-US dumps are available on Google Drive shared by iPassleader: <https://drive.google.com/open?id=1jEwVIVj0p8CoObh1Z59BWK2AXQbBar6a>

The exam outline will be changed according to the new policy every year, and the CIPP-US questions torrent and other teaching software, after the new exam outline, we will change according to the syllabus and the latest developments in theory and practice and revision of the corresponding changes, highly agree with outline. The CIPP-US Exam Questions are the perfect form of a complete set of teaching material, teaching outline will outline all the knowledge points covered, comprehensive and no dead angle for the CIPP-US candidates presents the proposition scope and trend of each year.

The CIPP-US Exam covers a wide range of topics related to privacy, including privacy laws and regulations in the United States, privacy program governance, information security, data breach management, and privacy risk management. CIPP-US exam is divided into multiple-choice questions and consists of 90 questions that must be answered in 2.5 hours. To pass the exam, candidates must score at least 300 out of 500 points. Certified Information Privacy Professional/United States (CIPP/US) certification is valid for two years and requires individuals to earn 20 continuing privacy education (CPE) credits to maintain their certification.

>> Pass CIPP-US Test <<

CIPP-US Valid Test Cost & CIPP-US Exam Sample Questions

Successful people are those who are willing to make efforts. If you have never experienced the wind and rain, you will never see the rainbow. Giving is proportional to the reward. Now, our CIPP-US study materials just need you spend less time, then your life will take place great changes. Our company has mastered the core technology of the CIPP-US Study Materials. What's more, your main purpose is to get the certificate quickly and easily. Our goal is to aid your preparation of the CIPP-US exam. Our study materials are an indispensable helper for you anyway. Please pay close attention to our CIPP-US study materials.

How much IAPP CIPP-US: Certified Information Privacy Professional/United States (CIPP/US) Exam cost

IAPP CIPP-US: Certified Information Privacy Professional/United States (CIPP/US) exam cost is \$550 USD and retake fees is \$375 USD, for more information please visit the official website.

IAPP Certified Information Privacy Professional/United States (CIPP/US) Sample Questions (Q165-Q170):

NEW QUESTION # 165

What type of material is exempt from an individual's right to disclosure under the Privacy Act?

- **A. Material reporting investigative efforts pertaining to the enforcement of criminal law.**
- B. Material requires by statute to be maintained and used solely for research purposes.
- C. Material used to determine potential collaboration with foreign governments in negotiation of trade deals.
- D. Material reporting investigative efforts to prevent unlawful persecution of an individual.

Answer: A

Explanation:

The Privacy Act allows agencies to exempt certain records from some of its provisions, including the right to disclosure, if the records fall within one of the categories specified in subsections (j) or (k) of the Act. One of these categories is records maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision. 5 U.S.C. § 552a (j) (2). Therefore, material reporting investigative efforts pertaining to the enforcement of criminal law falls within this category and can be exempted from the right to disclosure under the Privacy Act.

NEW QUESTION # 166

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 Fair and Accurate Credit Transactions Act (FACTA)
- D. The National Labor Relations Act (NLRA)

Answer: B

Explanation:

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

NEW QUESTION # 167

Which was NOT one of the five priority areas listed by the Federal Trade Commission in its 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"?

- A. Do Not Track
- B. Large platform providers
- C. Promoting enforceable self-regulatory codes
- **D. International data transfers**

Answer: D

NEW QUESTION # 168

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.

What is the most effective kind of training CloudHealth could have given its employees to help prevent this type of data breach?

- A. Training on the terms of the contractual agreement with HealthCo
- **B. Training on techniques for identifying phishing attempts**
- C. Training on the difference between confidential and non-public information
- D. Training on CloudHealth's HR policy regarding the role of employees involved data breaches

Answer: B

Explanation:

Phishing is a form of social engineering that involves sending fraudulent emails or other messages that appear to come from a legitimate source, but are designed to trick recipients into revealing sensitive information, such as passwords, account numbers, or personal identifiers¹. Phishing is one of the most common and effective methods of cyberattacks, and it can lead to data breaches, identity theft, ransomware infections, or other serious consequences². Therefore, training on how to recognize and avoid phishing attempts is crucial for any organization that handles sensitive data, especially ePHI, which is subject to strict regulations under HIPAA³.

Training on techniques for identifying phishing attempts can help employees to spot the signs of a phishing email, such as:

* Sender's address or domain name that does not match the expected source or contains spelling errors⁴

* Generic salutations or impersonal tone that do not address the recipient by name or use proper grammar⁴

- * Urgent or threatening language that creates a sense of pressure or fear and asks the recipient to take immediate action, such as clicking on a link, opening an attachment, or providing information⁴
 - * Suspicious links or attachments that may contain malware or lead to fake websites that mimic the appearance of a legitimate site, but have a different URL or request login credentials or other data⁴
 - * Requests for sensitive information that are unusual or out of context, such as asking for passwords, account numbers, or personal identifiers that the sender should already have or should not need⁴
- Training on techniques for identifying phishing attempts can also help employees to learn how to respond to a phishing email, such as:
- * Not clicking on any links or opening any attachments in the email⁴
 - * Not replying to the email or providing any information to the sender⁴
 - * Reporting the email to the IT department or security team and deleting it from the inbox⁴
 - * Verifying the legitimacy of the email by contacting the sender directly using a different channel, such as phone or another email address⁴
 - * Updating the antivirus software and scanning the device for any malware infection⁴
- Training on techniques for identifying phishing attempts is the most effective kind of training that CloudHealth could have given its employees to help prevent this type of data breach, because it would have enabled them to recognize the phishing email that compromised the PHI of more than 10,000 HealthCo patients, and to avoid falling victim to it. Training on the terms of the contractual agreement with HealthCo, the difference between confidential and non-public information, or CloudHealth's HR policy regarding the role of employees involved in data breaches, while important, would not have been as effective in preventing this specific type of data breach, because they would not have addressed the root cause of the breach, which was the phishing email.

References:

- * 1: IAPP, Phishing, <https://iapp.org/resources/glossary/phishing/>
- * 2: SpinOne, The Top 5 Phishing Awareness Training Providers 2023, <https://spinbackup.com/blog/phishing-awareness-training-best-providers/>
- * 3: IAPP, HIPAA, <https://iapp.org/resources/glossary/hipaa/>
- * 4: Expert Insights, The Top 11 Phishing Awareness Training and Simulation Solutions, <https://expertinsights.com/insights/the-top-11-phishing-awareness-training-and-simulation-solutions/>

NEW QUESTION # 169

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 followed internal notification procedures compatible with state law.
- D. If the entity was subject to the GLBA Safeguards Rule.

Answer: B

Explanation:

Most state breach notification laws require entities to notify affected individuals and/or regulators when there is unauthorized access to or acquisition of personal information that compromises its security, confidentiality, or integrity. However, some states provide exceptions to this requirement under certain conditions, such as:

- * If the data involved was encrypted or otherwise rendered unreadable or unusable, and the encryption key or other means of access was not compromised. This is based on the assumption that encrypted data is not accessible to unauthorized parties, even if they obtain the data.
- * If the entity was subject to and complied with another federal or state law that provides similar or greater protection and notification requirements, such as the GLBA Safeguards Rule or the HIPAA Breach Notification Rule. This is to avoid duplication or inconsistency of obligations for entities that are already regulated by other laws.
- * If the entity conducted a risk assessment and determined that there is no reasonable likelihood of harm to the affected individuals, based on factors such as the nature and extent of the data, the circumstances of the breach, the evidence of misuse, and the ability to mitigate the risk. This is to allow entities to exercise some discretion and judgment in evaluating the potential impact of the breach. However, none of the state laws provide an exception for the mere access of data without exportation. Access alone is considered a breach that triggers the notification requirement, unless one of the other conditions applies. Therefore, option B is not a sufficient excuse for not providing breach notification under state law.

References:

- * [IAPP CIPP/US Study Guide], Chapter 9: State Data Security Laws, pp. 209-211.
- * CIPP/US Practice Questions (Sample Questions), Question 29.

NEW QUESTION # 170

CIPP-US Valid Test Cost: <https://www.ipassleader.com/IAPP/CIPP-US-practice-exam-dumps.html>

- DOWNLOAD the newest iPassleader CIPP-US PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1jEwVIVj0p8CoObh1Z59BWK2AXObBar6a>

DOWNLOAD the newest iPassleader CIPP-US PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1jEwVIVj0p8CoObh1Z59BWK2AXObBar6a>