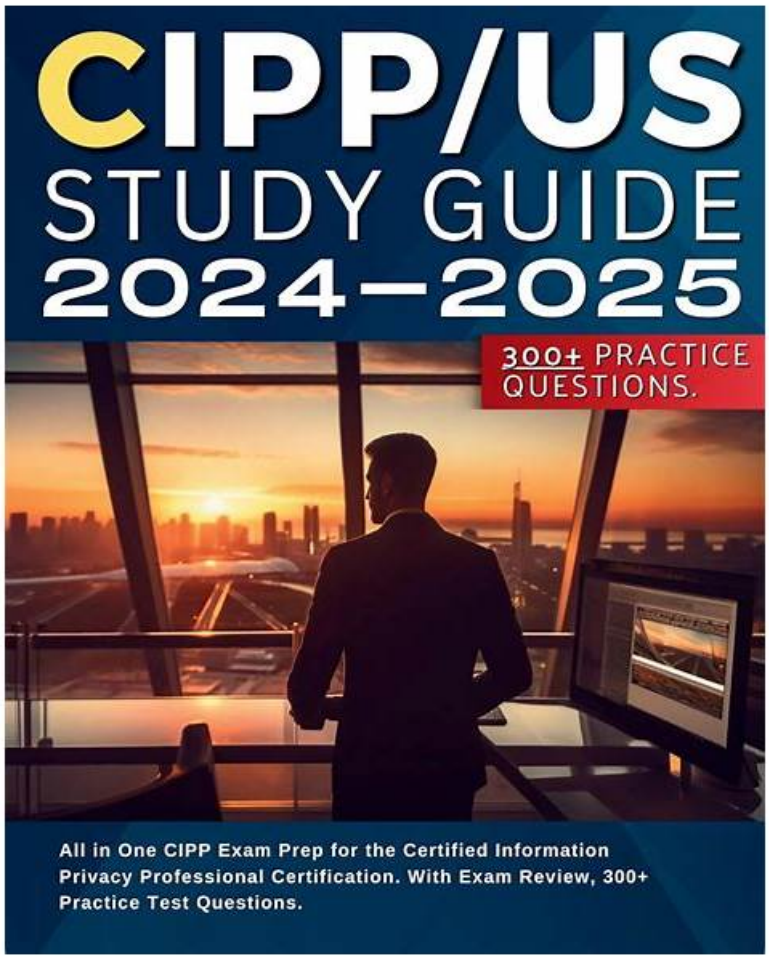
Study CIPP-US Center & New CIPP-US Exam Pdf



BONUS!!! Download part of ExamCost CIPP-US dumps for free: https://drive.google.com/open?id=1aHzkggeo8LTP7v026ZNazgVcXHeKlh52

Perhaps you worry about that you have difficulty in understanding our CIPP-US training questions. Frankly speaking, we have taken all your worries into account. Firstly, all knowledge of the CIPP-US exam materials have been simplified a lot. Also, we have tested many volunteers who are common people. The results show that our CIPP-US study braindumps are easy for them to understand. So you don't have to worry that at all and you will pass the exam for sure.

The CIPP-US Certification Exam is generally taken by professionals who work in the fields of privacy law, information security, data management, and compliance. CIPP-US exam is also suitable for individuals who work in the areas of data protection and privacy in organizations such as law firms, consulting firms, and other companies that deal with sensitive data. Certified Information Privacy Professional/United States (CIPP/US) certification is also suitable for individuals who work in government agencies that deal with data privacy and protection.

>> Study CIPP-US Center <<

Study CIPP-US Center 100% Pass | Reliable CIPP-US: Certified Information Privacy Professional/United States (CIPP/US) 100% Pass

Many applicants do not fulfill their dream of becoming professionals because of using outdated exam preparation material. Failure in the Certified Information Privacy Professional/United States (CIPP/US) exam leads them to anxiety. If this situation sounds familiar, do not waste time and get your hands on IAPP CIPP-US for exam preparation.

The CIPP-US Exam consists of 90 multiple-choice questions and lasts for two and a half hours. To prepare for the exam, candidates should have a solid foundation in privacy law and regulations, data security practices, and privacy management

frameworks. This can be achieved through classroom training, self-study, and practice exams.

IAPP Certified Information Privacy Professional/United States (CIPP/US) Sample Questions (Q175-Q180):

NEW QUESTION # 175
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 mentionedthis 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 definition of tort law
- C. The strict nature of state law
- D. The enforceability of local law

Answer: A

Explanation:
Larry has a misconception about the applicability of federal law to private-sector employee rights. He believes that the U.S. Constitution protects American workers from various forms of discrimination, harassment, and invasion of privacy by their employers. However, the U.S. Constitution only applies to government actions, not private actions, unless there is a specific federal statute that extends constitutional protections to the private sector1. For example, the Civil Rights Act of 1964 prohibits discrimination on the basis of race, color, religion, sex, or national origin by private employers2. The Electronic Communications Privacy Act of 1986 regulates the interception and disclosure of electronic communications by private parties3. The CAN-SPAM Act of 2003 sets the rules for commercial email and gives recipients the right to opt out of receiving unwanted messages4. These are examples of federal laws that apply to private-sector employees, but they do not cover all the situations that Larry faces at SunriseLynx. For instance, there is no federal law that protects private-sector employees from political discrimination or from having their personal mail opened by their employers. Larry may have to rely on state laws or common law torts to seek redress for these violations of his rights. References: 1: Private Sector vs. Public Sector Employee Rights2: [Civil Rights Act of 1964 - Wikipedia] 3: [Electronic Communications Privacy Act - Wikipedia] 4: CAN-SPAM Act: A Compliance Guide for Business : IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 5:
Federal Trade Commission and Consumer Privacy, p. 141-142

NEW QUESTION # 176
A law enforcement subpoenas the ACME telecommunications company for access to text message records of a person suspected of planning a terrorist attack. The company had previously encrypted its text message records so that only the suspect could access this data.
What law did ACME violate by designing the service to prevent access to the information by a law enforcement agency?

- A. USA Freedom Act
- B. ECPA
- C. CALEA
- D. SCA

Answer: C

Explanation:
The law that ACME violated by designing the service to prevent access to the information by a law enforcement agency is the Communications Assistance for Law Enforcement Act (CALEA)1. CALEA is a federal law that requires telecommunications carriers and manufacturers of telecommunications equipment to design their equipment, facilities, and services to ensure that they have the necessarysurveillance capabilities to comply with legal requests for interception of communications2. CALEA applies to all commercial messages, including text messages, and gives law enforcement agencies the authority to subpoena the records of such communications from the service providers3. By encrypting its text message records so that only the suspect could access this data, ACME violated CALEA's duty to cooperate in the interception of communications for law enforcement purposes. References: 1: Communications Assistance for Law Enforcement Act - Wikipedia2: Home | CALEA | The Commission on Accreditation for Law Enforcement Agencies, Inc.3: Communications Assistance for Law Enforcement Act : IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 6: Law Enforcement and National Security Access, p. 177

NEW QUESTION # 177
Smith Memorial Healthcare (SMH) is a hospital network headquartered in New York and operating in 7 other states. SMH uses an electronic medical record to enter and track information about its patients. Recently, SMH suffered a data breach where a third-party hacker was able to gain access to the SMH internal network.
Because it is a HIPPA-covered entity, SMH made a notification to the Office of Civil Rights at the U.S. Department of Health and Human Services about the breach.
Which statement accurately describes SMH's notification responsibilities?

- A. If SMH must make a notification in any other state in which it operates, it must also make a notification to individuals in New York.
- B. If SMH has more than 500 patients in the state of New York, it will need to make separate notifications to these patients.
- C. If SMH makes credit monitoring available to individuals who inquire, it will not have to make a separate
- D. If SMH is compliant with HIPAA, it will not have to make a separate notification to individuals in the state of New York.

Answer: D

Explanation:
notification to individuals in the state of New York.
Explanation:
https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart-new-york.html

NEW QUESTION # 178
What is the main purpose of requiring marketers to use the Wireless Domain Registry?

- A. To ensure their emails are sent to actual wireless subscribers
- B. To acquire authorization to send emails to mobile devices
- C. To access a current list of wireless domain names
- D. To prevent unauthorized emails to mobile devices

Answer: D

Explanation:
The Wireless Domain Registry is a list of domain names that are used to transmit electronic messages to wireless devices, such as cell phones and pagers. The purpose of the registry is to protect wireless consumers from unwanted commercial electronic mail messages, by identifying the domain names for those who send such messages. Marketers are required to use the registry to avoid sending unsolicited emails to wireless devices, which may incur costs or inconvenience for the recipients. Sending such emails without the express prior authorization of the recipient is a violation of the CAN-SPAM Act of 2003. References: https://www.fcc.gov/cgb/policy/domain-name-input
https://www.prnewswire.com/in/news-releases/the-wireless-registry-launches-worlds-first-global- registry-for-wireless-names-240222521.html

NEW QUESTION # 179
Even when dealing with an organization subject to the CCPA, California residents are NOT legally entitled to request that the organization do what?

- A. Disclose their personal information to them.
- B. Delete their personal information.
- C. Correct their personal information.
- D. Refrain from selling their personal information to third parties.

Answer: C

Explanation:
The CCPA grants California residents the right to request that a business delete, disclose, or stop selling their personal information, but it does not grant them the right to request that a business correct their personal information. However, the CPRA, which will amend and expand the CCPA in 2023, will grant California residents the right to request that a business correct inaccurate personal information.

NEW QUESTION # 180
.....

id=1aHzkggeo8LTP7v026ZNazgVcXHeKlh52