DUMPSARENA

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

IAPP CIPP-US

Version Demo

Total Demo Questions: 10

Total Premium Questions: 164

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 1

What does the Massachusetts Personal Information Security Regulation require as it relates to encryption of personal information?

A. The encryption of all personal information of Massachusetts residents when all equipment is located in Massachusetts.

B. The encryption of all personal information stored in Massachusetts-based companies when all equipment is located in Massachusetts.

C. The encryption of personal information stored in Massachusetts-based companies when stored on portable devices.

D. The encryption of all personal information of Massachusetts residents when stored on portable devices.

ANSWER: D

Explanation:

Reference: https://www.dataguidance.com/notes/massachusetts-data-protection-overview

QUESTION NO: 2

What consumer service was the Fair Credit Reporting Act (FCRA) originally intended to provide?

A. The ability to receive reports from multiple credit reporting agencies.

B. The ability to appeal negative credit-based decisions.

C. The ability to correct inaccurate credit information.

D. The ability to investigate incidents of identity theft.

ANSWER: D

Explanation:

Reference: https://epic.org/privacy/fcra/

QUESTION NO: 3

Which entities must comply with the Telemarketing Sales Rule?

A. For-profit organizations and for-profit telefunders 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 NO: 4

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.

Based on the way he uses social media, Evan is susceptible to a lawsuit based on?

A. Defamation

B. Discrimination

C. Intrusion upon seclusion

D. Publicity given to private life

ANSWER: B

QUESTION NO: 5

Which statute is considered part of U.S. federal privacy law?

A. The Fair Credit Reporting Act.

B. SB 1386.

C. The Personal Information Protection and Electronic Documents Act.

D. The e-Privacy Directive.

ANSWER: A

Explanation:

Reference: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

QUESTION NO: 6

Which of these organizations would be required to provide its customers with an annual privacy notice?

A. The Four Winds Tribal College.

B. The Golden Gavel Auction House.

C. The King County Savings and Loan.

D. The Breezy City Housing Commission.

ANSWER: B

QUESTION NO: 7

Privacy Is Hiring Inc., a CA-based company, is an online specialty recruiting firm focusing on placing privacy professionals in roles at major companies. Job candidates create online profiles

outlining their experience and credentials, and can pay $19.99/month via credit card to have their profiles promoted to potential employers. Privacy Is Hiring Inc. keeps all customer data at rest encrypted on its servers.

Under what circumstances would Privacy Is Hiring Inc., need to notify affected individuals in the event of a data breach?

A. If law enforcement has completed its investigation and has authorized Privacy Is Hiring Inc. to provide the notification to clients and applicable regulators.

B. If the job candidates' credit card information and the encryption keys were among the information taken.

C. If Privacy Is Hiring Inc., reasonably believes that job candidates will be harmed by the data breach.

D. If the personal information stolen included the individuals' names and credit card pin numbers.

ANSWER: D

QUESTION NO: 8

Which is an exception to the general prohibitions on telephone monitoring that exist under the U.S. Wiretap Act?

A. Call center exception

B. Inter-company communications exception

C. Ordinary course of business exception

D. Internet calls exception

ANSWER: C

Explanation:

Reference: https://www.lexology.com/library/detail.aspx?g=1031d6a6-19f5-4422-b5a2-98d7038905e9

QUESTION NO: 9

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 thirdparty 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
Because HealthCo did not require CloudHealth to implement appropriate physical and administrative measures to safeguard the ePHI

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 significant reason that the U.S. Department of Health and Human Services (HHS) might impose a penalty on HealthCo?
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 NO: 10

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

ANSWER: A

DUMPSARENA