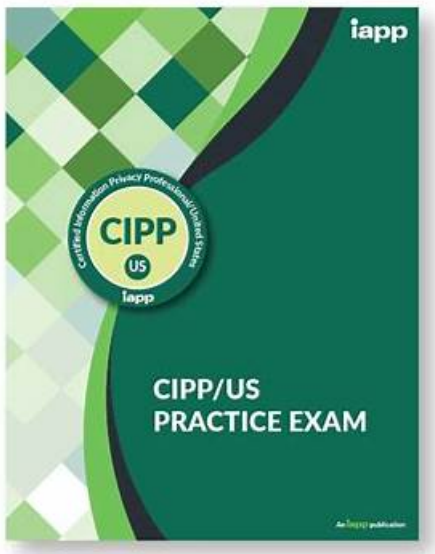
High Pass-Rate IAPP Pdf CIPP-US Format & Trustable RealValidExam - Leading Provider in Qualification Exams



BONUS!!! Download part of RealValidExam CIPP-US dumps for free: https://drive.google.com/open?id=1yX-x0QAV4Gd6_1H9l0sSjFsd0NgbQgSe

If you want to understand our CIPP-US exam prep, you can download the demo from our web page. You do not need to spend money; because our CIPP-US test questions provide you with the demo for free. You just need to download the demo of our CIPP-US exam prep according to our guiding; you will get the demo for free easily before you purchase our products. By using the demo, we believe that you will have a deeply understanding of our CIPP-US Test Torrent. We can make sure that you will like our products; because you will it can help you a lot.

Target Audience

This evaluation is designed for data protection officials in the US or those who wish to obtain awareness of how such policies work in the US. The exam, in particular, tests their knowledge and understanding in the field and helps them determine the areas they have to work on. It is also ideal for specialists who want to get the affiliated designation.

>> Pdf CIPP-US Format <<

Latest CIPP-US Questions | Study CIPP-US Material

It is universally accepted that the competition in the labor market has become more and more competitive in the past years. In order to gain some competitive advantages, a growing number of people have tried their best to pass the CIPP-US exam. Because a lot of people hope to get the certification by the related exam, now many leaders of companies prefer to the candidates who have the CIPP-US Certification. In their opinions, the certification is a best reflection of the candidates' work ability, so more and more leaders of companies start to pay more attention to the CIPP-US certification of these candidates.

The IAPP CIPP-US exam covers a wide range of topics related to data privacy, including key U.S. privacy laws such as HIPAA, COPPA, GLBA, and the California Consumer Privacy Act (CCPA). It also covers topics such as data breach notification

requirements, privacy program management, and privacy impact assessments. Achieving the CIPP-US certification demonstrates a candidate's commitment to the field of data privacy and their ability to provide expert advice and guidance to organizations on privacy matters.

The CIPP-US certification exam is designed for privacy professionals who are involved in the collection, use, and dissemination of personal data in the United States. Certified Information Privacy Professional/United States (CIPP/US) certification program is ideal for privacy professionals who work in industries such as healthcare, finance, technology, and retail, among others. CIPP-US Exam covers various topics such as the U.S. legal system, the privacy framework, privacy principles and practices, and data protection technologies.

IAPP Certified Information Privacy Professional/United States (CIPP/US) Sample Questions (Q97-Q102):

NEW QUESTION # 97
SCENARIO
Please use the following to answer the next QUESTION:
Matt went into his son's bedroom one evening and found him stretched out on his bed typing on his laptop. "Doing your network?" Matt asked hopefully.
"No," the boy said. "I'm filling out a survey."
Matt looked over his son's shoulder at his computer screen. "What kind of survey?" "It's asking Questions about my opinions."
"Let me see," Matt said, and began reading the list of Questions that his son had already answered. "It's asking your opinions about the government and citizenship. That's a little odd. You're only ten." Matt wondered how the web link to the survey had ended up in his son's email inbox. Thinking the message might have been sent to his son by mistake he opened it and read it. It had come from an entity called the Leadership Project, and the content and the graphics indicated that it was intended for children. As Matt read further he learned that kids who took the survey were automatically registered in a contest to win the first book in a series about famous leaders.
To Matt, this clearly seemed like a marketing ploy to solicit goods and services to children. He asked his son if he had been prompted to give information about himself in order to take the survey. His son told him he had been asked to give his name, address, telephone number, and date of birth, and to answer Questions about his favorite games and toys.
Matt was concerned. He doubted if it was legal for the marketer to collect information from his son in the way that it was. Then he noticed several other commercial emails from marketers advertising products for children in his son's inbox, and he decided it was time to report the incident to the proper authorities.
How does Matt come to the decision to report the marketer's activities?

- A. The marketer failed to make an adequate attempt to provide Matt with information
- B. The marketer did not provide evidence that the prize books were appropriate for children
- C. The marketer seems to have distributed his son's information without Matt's permission
- D. The marketer failed to identify himself and indicate the purpose of the messages

Answer: A

NEW QUESTION # 98
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 aresult of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.
Of the safeguards required by the HIPAA Security Rule, which of the following is NOT at issue due to HealthCo's actions?

- A. Technical Safeguards
- B. Physical Safeguards
- C. Security Safeguards
- D. Administrative Safeguards

Answer: C

Explanation:
The HIPAA Security Rule requires covered entities and their business associates to implement three types of safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI): administrative, physical, and technical1. Security safeguards is not a separate category of safeguards, but rather a general term that encompasses all three types. Therefore, it is not a correct answer to the question.
* Administrative safeguards are the policies and procedures that govern the conduct of the workforce and the security measures put in place to protect ePHI. They include risk analysis and management, training, contingency planning, incident response, and evaluation12.
* Physical safeguards are the locks, doors, cameras, and other physical measures that prevent unauthorized access to ePHI. They include workstation and device security, locks and keys, and disposal of media12.
* Technical safeguards are the software and hardware tools that protect ePHI from unauthorized access, alteration, or destruction. They include access control, encryption, audit controls, integrity controls, and transmission security12.
In the scenario, HealthCo's actions have potentially violated all three types of safeguards. For example:
* HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures. This could be a breach of the administrative safeguard of risk analysis and management12.
* HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. This could be a breach of the technical safeguard of encryption12.
* HealthCo provides its investigative report of the breach and a copy of the PHI of the individuals affected to law enforcement. This could be a breach of the physical safeguard of disposal of media, if HealthCo did not ensure that the media was properly erased or destroyed after the transfer12.
References: 1: Summary of the HIPAA Security Rule, HHS.gov. 2: What is the HIPAA Security Rule?
Safeguards ... - Secureframe, Secureframe.com.

NEW QUESTION # 99
Which of the following became the first state to pass a law specifically regulating the collection of biometric data?

- A. Washington.
- B. Illinois.
- C. California.
- D. Texas.

Answer: B

NEW QUESTION # 100
Which of the following became the first state to pass a law specifically regulating the collection of biometric data?

- A. Washington.
- B. Illinois.
- C. California.
- D. Texas.

Answer: B

Explanation:
Illinois became the first state to pass a law specifically regulating the collection of biometric data in 2008, when it enacted the Biometric Information Privacy Act (BIPA). BIPA defines biometric identifiers as retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry, and biometric information as any information based on biometric identifiers used to identify an individual. BIPA requires entities that collect, store, or use biometric identifiers or information to obtain informed consent from

individuals, provide written policies on data retention and destruction, limit disclosure and sale of biometric data, and protect biometric data using reasonable security measures. BIPA also provides a private right of action for individuals whose biometric data is collected, stored, or used in violation of the law, and allows them to recover statutory damages of $1,000 or actual damages, whichever is greater, for each negligent violation, and $5,000 or actual damages, whichever is greater, for each intentional or reckless violation, as well as attorneys' fees and costs, and injunctive relief.

NEW QUESTION # 101
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 significant reason that the U.S. Department of Health and Human Services (HHS) might impose a penalty on HealthCo?

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

Answer: C

Explanation:
According to the HIPAA Security Rule, covered entities are responsible for ensuring that their business associates comply with the security standards and safeguards required by the rule. This includes conducting due diligence to assess the business associate's security capabilities and practices, and monitoring their performance and compliance. Failure to do so may result in a violation of the rule and a penalty by the HHS.
In this scenario, HealthCo did not perform due diligence on CloudHealth before entering the contract, and did not conduct audits of CloudHealth's security measures. This is the most significant reason why HHS might impose a penalty on HealthCo, as it indicates a lack of oversight and accountability for the protection of ePHI. References:
* HIPAA Security Rule
* HIPAA Business Associate Contracts
* HIPAA Enforcement and Penalties

NEW QUESTION # 102
.....

□ for free by simply searching on 「 www.examdiscuss.com 」 □CIPP-US Sample Questions

- CIPP-US Reliable Exam Cost □ New CIPP-US Test Guide Ⓜ CIPP-US Lab Questions □ Search for ▹ CIPP-US ◃ and download it for free immediately on ⇛ www.pdfvce.com ⇚ □Exam CIPP-US Certification Cost
- CIPP-US Reliable Exam Cost □ CIPP-US Valid Test Book □ Real CIPP-US Dumps □ Enter 「 www.prepawayexam.com 」 and search for ➥ CIPP-US □ to download for free □CIPP-US Reliable Exam Cost
- Reliable CIPP-US Exam Question □ CIPP-US Latest Study Materials □ Reliable CIPP-US Exam Question □ ➤ www.pdfvce.com □ is best website to obtain 【 CIPP-US 】 for free download □CIPP-US Reliable Exam Cost
- CIPP-US Online Exam □ CIPP-US Valid Test Book □ Exam CIPP-US Certification Cost □ Search for ☀ CIPP-US □☀□ and download it for free immediately on ▸ www.prepawayete.com ◂ □Real CIPP-US Dumps
- CIPP-US Certified Information Privacy Professional/United States (CIPP/US) For Guaranteed Success □ Search for 《 CIPP-US 》 and easily obtain a free download on ▸ www.pdfvce.com ◂ □CIPP-US Sample Questions
- Is IAPP CIPP-US Questions – Best Way To Clear The Exam? □ Enter ⇛ www.validtorrent.com ⇚ and search for ⇛ CIPP-US ⇚ to download for free □CIPP-US Lab Questions
- Exam CIPP-US Certification Cost □ CIPP-US Valid Test Book □ CIPP-US Reliable Exam Cost □ Search for ✔ CIPP-US □✔□ and download it for free immediately on 【 www.pdfvce.com 】 □CIPP-US Pass4sure Exam Prep
- Practice CIPP-US Exam □ CIPP-US Online Exam □ Reliable CIPP-US Exam Question □ □ www.practicevce.com □ is best website to obtain " CIPP-US " for free download □Practice CIPP-US Exam
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New CIPP-US dumps are available on Google Drive shared by RealValidExam: https://drive.google.com/open?id=1yX-x0QAV4Gd6_1H9l0sSjFsd0NgbQgSe