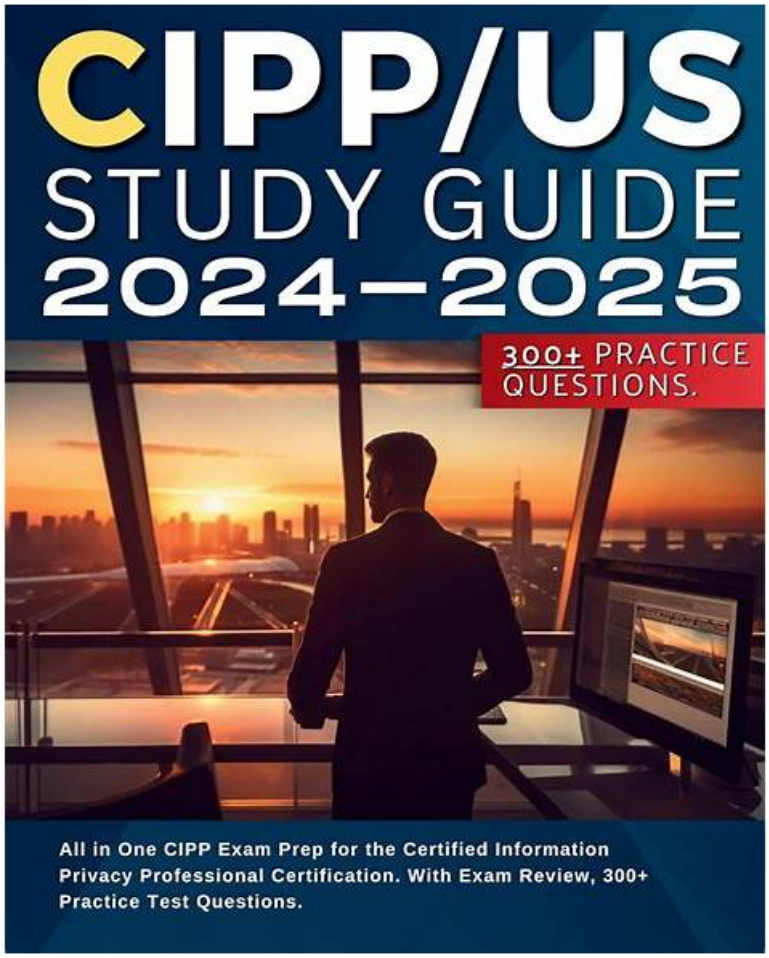
시험대비CIPP-US퍼펙트최신덤프공부최신덤프모음집



그리고 Itcertkr CIPP-US 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1OkNvLu748b38TvgTBVSk3SFEabUSNimC

IAPP CIPP-US 덤프구매전 한국어 온라인상담서비스부터 구매후 덤프 무료 업데이트버전제공 , IAPP CIPP-US시험불합격시 덤프비용 전액환불 혹은 다른 과목으로 교환 등 저희는 구매전부터 구매후까지 철저한 서비스를 제공해드립니다. IAPP CIPP-US 덤프는 인기덤프인데 지금까지 덤프를 구매한후 환불신청하신 분은 아직 없었습니다.

IAPP CIPP-US (Certified Information Privacy Professional/United States) 시험은 데이터 프라이버시 분야의 전문가에게 매우 존경받는 인증입니다. 이 인증은 국제 개인 정보 보호 전문가 (IAPP)가 수여하는데, 이는 개인 정보 보호 전문가를위한 가장 크고 가장 존경받는 글로벌 협회 인 IAPP (International Association of Privacy Professionals)가 수여합니다. CIPP-US 시험은 미국의 개인 정보 보호법 및 규정에 대한 후보자의 지식과 조직에서 개인 정보 보호 프로그램을 구현하고 관리하는 능력을 테스트하도록 설계되었습니다.

CIPP-US 자격증 시험은 미국 연방 및 주 개인 정보 보호 법률, 규정 및 업계 최상의 관행 등의 다양한 주제를 다루고 있습니다. 이 자격증을 소지한 전문가들은 복잡한 규제 환경을 탐색하고 데이터 보호 법률을 준수하는 데 잘 준비돼 있습니다. 또한 그들은 자신의 분야에서 전문가로 인정받아 경력 기회를 높일 수 있습니다.

IAPP CIPP-US 시험은 데이터 프라이버시 분야에서 일하는 모든 사람들에게 필수적인 구성 요소입니다. 개인 정보 보호 컨설턴트, 변호사 또는 내부 개인 정보 보호 팀 구성원이던, CIPP-US 자격증은 전문적인 신뢰성과 효과성을 향상시킬 가치 있는 자격증입니다.

>> CIPP-US퍼펙트 최신 덤프공부 <<

시험대비 CIPP-US퍼펙트 최신 덤프공부 덤프공부

Itcertkr의 IAPP CIPP-US 덤프로 시험을 준비하면IAPP CIPP-US시험패스를 예약한것과 같습니다. 가장 최근 출제된 IAPP CIPP-US시험문제를 바탕으로 만들어진 적중율 최고인 덤프로서 간단한 시험패스는 더는 꿈이 아닙니다. 덤프는 pdf파일과 온라인서비스로 되어있는데 pdf버전은 출력가능하고 온라인버전은 휴대폰에서도 작동가능합니다.

최신 Certified Information Privacy Professional CIPP-US 무료샘플문제 (Q106-Q111):

질문 # 106
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.
Of the safeguards required by the HIPAA Security Rule, which of the following is NOT at issue due to HealthCo's actions?

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

정답：D

질문 # 107
Under state breach notification laws, which is NOT typically included in the definition of personal information?

- A. Social Security number
- B. State identification number
- C. First and last name
- D. Medical Information

정답：C

설명:
Under state breach notification laws, personal information is typically defined as an individual's first name or first initial and last name plus one or more other data elements, such as Social Security number, state identification number, account number, medical information, etc. However, first and last name alone are not usually considered personal information, unless they are combined with other data elements that could identify the individual or compromise their security or privacy. Therefore, option B is the correct answer, as it is not typically included in the definition of personal information under state breach notification laws. References: https://www.ncsl.org/technology-and-communication/security-breach-notification-lawshttps://

질문 # 108
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 HealthCo did not conduct due diligence to verify or monitor CloudHealth's security measures
- B. Because CloudHealth violated its contract with HealthCo by not encrypting the ePHI
- C. Because HealthCo did not require CloudHealth to implement appropriate physical and administrative measures to safeguard the ePHI
- D. Because HIPAA requires the imposition of a fine if a data breach of this magnitude has occurred

정답：A

질문 # 109
Which act violates the Family Educational Rights and Privacy Act of 1974 (FERPA)?

- A. A university posts a public student directory that includes names, hometowns, e-mail addresses, and majors
- B. University police provide an arrest report to a student's hometown police, who suspect him of a similar crime
- C. A newspaper prints the names, grade levels, and hometowns of students who made the quarterly honor roll
- D. A K-12 assessment vendor obtains a student's signed essay about her hometown from her school to use as an exemplar for public release

정답：D

질문 # 110
Which of the following best describes how federal anti-discrimination laws protect the privacy of private- sector employees in the United States?

- A. They limit the amount of time a potential employee can be interviewed.
- B. They promote a workforce of employees with diverse skills and interests.
- C. They prescribe working environments that are safe and comfortable.
- D. They limit the types of information that employers can collect about employees.

정답：D

설명：
Federal anti-discrimination laws, such as Title VII of the Civil Rights Act of 1964, the Equal Pay Act of 1963, the Age Discrimination in Employment Act of 1967, and the Americans with Disabilities Act of 1990, prohibit employers from discriminating against employees or applicants based on certain protected characteristics, such as race, color, religion, sex, national origin, age, disability, and genetic information.
These laws also limit the types of information that employers can collect, use, disclose, or retain about employees or applicants, in order to prevent discrimination or invasion of privacy. For example, employers cannot ask about an applicant's medical history, disability status, genetic information, or religious beliefs, unless they are relevant to the job or a bona fide occupational qualification. Employers also cannot use such information to make adverse employment decisions, such as hiring, firing, promotion, or

compensation, unless they are justified by a legitimate business necessity or a reasonable accommodation. Employers must also safeguard the confidentiality of such information and dispose of it properly when it is no longer needed. References:
* Federal Laws Prohibiting Job Discrimination Questions And Answers
* Laws Enforced by EEOC
* Employment and Anti-Discrimination Laws in the Workplace
* Protections Against Discrimination and Other Prohibited Practices
* 3. Who is protected from employment discrimination?

질문 # 111
......

많은 시간과 돈이 필요 없습니다. 30분이란 특별학습가이드로 여러분은IAPP CIPP-US인증시험을 한번에 통과할 수 있습니다, Itcertkr에서IAPP CIPP-US시험자료의 문제와 답이 실제시험의 문제와 답과 아주 비슷한 덤프만 제공합니다.