



CIPP-US^{Q&As}

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

Pass IAPP CIPP-US Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/cipp-us.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

SCENARIO

Please use the following to answer the next question:

Declan has just started a job as a nursing assistant in a radiology department at Woodland Hospital. He has also started a program to become a registered nurse.

Before taking this career path, Declan was vaguely familiar with the Health Insurance Portability and Accountability Act (HIPAA). He now knows that he must help ensure the security of his patients' Protected Health Information (PHI).

Therefore, he is thinking carefully about privacy issues.

On the morning of his first day, Declan noticed that the newly hired receptionist handed each patient a HIPAA privacy notice. He wondered if it was necessary to give these privacy notices to returning patients, and if the radiology department

could reduce paper waste through a system of one-time distribution.

He was also curious about the hospital's use of a billing company. He questioned whether the hospital was doing all it could to protect the privacy of its patients if the billing company had details about patients' care.

On his first day Declan became familiar with all areas of the hospital's large radiology department. As he was organizing equipment left in the hallway, he overheard a conversation between two hospital administrators. He was surprised to

hear that a portable hard drive containing non-encrypted patient information was missing. The administrators expressed relief that the hospital would be able to avoid liability. Declan was surprised, and wondered whether the hospital had

plans to properly report what had happened.

Despite Declan's concern about this issue, he was amazed by the hospital's effort to integrate Electronic Health Records (EHRs) into the everyday care of patients. He thought about the potential for streamlining care even more if they were

accessible to all medical facilities nationwide.

Declan had many positive interactions with patients. At the end of his first day, he spoke to one patient, John, whose father had just been diagnosed with a degenerative muscular disease. John was about to get blood work done, and he

feared that the blood work could reveal a genetic predisposition to the disease that could affect his ability to obtain insurance coverage. Declan told John that he did not think that was possible, but the patient was wheeled away before he

could explain why. John plans to ask a colleague about this.

In one month, Declan has a paper due for one of his classes on a health topic of his choice. By then, he will have had many interactions with patients he can use as examples. He will be pleased to give credit to John by name for inspiring him to

think more carefully about genetic testing.

Although Declan's day ended with many questions, he was pleased about his new position.



How can the radiology department address Declan's concern about paper waste and still comply with the Health Insurance Portability and Accountability Act (HIPAA)?

- A. State the privacy policy to the patient verbally
- B. Post the privacy notice in a prominent location instead
- C. Direct patients to the correct area of the hospital website
- D. Confirm that patients are given the privacy notice on their first visit

Correct Answer: D

D: "Privacy notices. The Privacy Rule generally requires a covered entity to provide a detailed privacy notice at the date of first service delivery. There are some defined exceptions to the notice requirements. For example, a privacy notice does not have to be provided when the healthcare provider has an "indirect treatment relationship" with the patient or in the case of medical emergencies. The rule is quite specific about elements that must be included in the notice, including detailed statements about individuals' rights with respect to their PHI."

QUESTION 2

Which of the following best describes the ASIA-Pacific Economic Cooperation (APEC) principles?

- A. A bill of rights for individuals seeking access to their personal information.
- B. A code of responsibilities for medical establishments to uphold privacy laws.
- C. An international court ruling on personal information held in the commercial sector.
- D. A baseline of marketers' minimum responsibilities for providing opt-out mechanisms.

Correct Answer: A

Reference: <http://documents1.worldbank.org/curated/en/751621525705087132/text/WPS8431.txt>

QUESTION 3

SCENARIO

Please use the following to answer the next question:

Jane is a U.S. citizen and a senior software engineer at California-based Jones Labs, a major software supplier to the U.S. Department of Defense and other U.S. federal agencies. Jane's manager, Patrick, is a French citizen who has been living in California for over a decade. Patrick has recently begun to suspect that Jane is an insider secretly transmitting trade secrets to foreign intelligence. Unbeknownst to Patrick, the FBI has already received a hint from anonymous whistleblower, and jointly with the National Security Agency is investigating Jane's possible implication in a sophisticated foreign espionage campaign.

Ever since the pandemic, Jane has been working from home. To complete her daily tasks she uses her corporate laptop, which after each login conspicuously provides notice that the equipment belongs to Jones Labs and may be monitored according to the enacted privacy policy and employment handbook. Jane also has a corporate mobile phone that she uses strictly for business, the terms of which are defined in her employment contract and elaborated upon in her employee handbook. Both the privacy policy and the employee handbook are revised annually by a reputable California



law firm specializing in privacy law. Jane also has a personal iPhone that she uses for private purposes only.

Jones Labs has its primary data center in San Francisco, which is managed internally by Jones Labs engineers. The secondary data center, managed by Amazon AWS, is physically located in the UK for disaster recovery purposes. Jones Labs' mobile devices backup is managed by a mid-sized mobile defense company located in Denver, which physically stores the data in Canada to reduce costs. Jones Labs' Microsoft Office documents are securely stored in a Microsoft Office 365 data center based in Ireland. Manufacturing data of Jones Labs is stored in Taiwan and managed by a local supplier that has no presence in the U.S.

When storing Jane's fingerprint for remote authentication, Jones Labs should consider legality issues under which of the following?

- A. The Privacy Rule of the HITECH Act.
- B. The California IoT Security Law (SB 327).
- C. The applicable state law such as Illinois BIPA.
- D. The federal Genetic Information Nondiscrimination Act (GINA).

Correct Answer: C

QUESTION 4

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 techniques for identifying phishing attempts
- B. Training on the terms of the contractual agreement with HealthCo
- 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

Correct Answer: A

QUESTION 5

Which statement is FALSE regarding the provisions of the Employee Polygraph Protection Act of 1988 (EPPA)?

- A. The EPPA requires that employers post essential information about the Act in a conspicuous location.
- B. The EPPA includes an exception that allows polygraph tests in professions in which employee honesty is necessary for public safety.
- C. Employers are prohibited from administering psychological testing based on personality traits such as honesty, preferences or habits.
- D. Employers involved in the manufacture of controlled substances may terminate employees based on polygraph results if other evidence exists.

Correct Answer: C

Reference: <https://hawleytroxell.com/2019/01/psychological-exams-and-personality-tests-in-employment-a-fine-line/>

[CIPP-US PDF Dumps](#)

[CIPP-US VCE Dumps](#)

[CIPP-US Practice Test](#)