



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.

What is the most likely way that Declan might directly violate the Health Insurance Portability and Accountability Act (HIPAA)?

- A. By being present when patients are checking in
- B. By speaking to a patient without prior authorization
- C. By ignoring the conversation about a potential breach



D. By following through with his plans for his upcoming paper

Correct Answer: D

"Other than for treatment, covered entities must make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary in order to accomplish the intended purpose." He isn't involved in the potential breach, which is why he isn't trained for it, and doesn't know all the facts of the situation. He has no obligation and doesn't need to investigate any further based on anything that he heard.

QUESTION 2

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 an 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 MS 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 3

SCENARIO



Please use the following to answer the next question:

When there was a data breach involving customer personal and financial information at a large retail store, the company's directors were shocked. However, Roberta, a privacy analyst at the company and a victim of identity theft herself, was

not. Prior to the breach, she had been working on a privacy program report for the executives. How the company shared and handled data across its organization was a major concern. There were neither adequate rules about access to

customer information nor

procedures for purging and destroying outdated data. In her research, Roberta had discovered that even low-level employees had access to all of the company's customer data, including financial records, and that the company still had in its

possession obsolete customer data going back to the 1980s.

Her report recommended three main reforms. First, permit access on an as-needs-to-know basis. This would mean restricting employees' access to customer information to data that was relevant to the work performed. Second, create a

highly secure database for storing customers' financial information (e.g., credit card and bank account numbers) separate from less sensitive information. Third, identify outdated customer information and then develop a process for securely

disposing of it.

When the breach occurred, the company's executives called Roberta to a meeting where she presented the recommendations in her report. She explained that the company having a national customer base meant it would have to ensure that

it complied with all relevant state breach notification laws. Thanks to Roberta's guidance, the company was able to notify customers quickly and within the specific timeframes set by state breach notification laws.

Soon after, the executives approved the changes to the privacy program that Roberta recommended in her report. The privacy program is far more effective now because of these changes and, also, because privacy and security are now

considered the responsibility of every employee.

Which principle of the Consumer Privacy Bill of Rights, if adopted, would best reform the company's privacy program?

- A. Consumers have a right to exercise control over how companies use their personal data.
- B. Consumers have a right to reasonable limits on the personal data that a company retains.
- C. Consumers have a right to easily accessible information about privacy and security practices.
- D. Consumers have a right to correct personal data in a manner that is appropriate to the sensitivity.

Correct Answer: B

QUESTION 4

A financial services company install "bossware" software on its employees' remote computers to monitor performance. The software logs screenshots, mouse movements, and keystrokes to determine whether an employee is being



productive. The software can also enable the computer webcams to record video footage.

Which of the following would best support an employee claim for an intrusion upon seclusion tort?

- A. The webcam is enabled to record video any time the computer is turned on.
- B. The company creates and saves a biometric template for each employee based upon keystroke dynamics.
- C. The software automatically sends a notification to a supervisor any time the employee's mouse is dormant for more than five minutes.
- D. The webcam records video of an employee using a company laptop to perform personal business while at a coffee shop during work hours.

Correct Answer: D

QUESTION 5

When developing a company privacy program, which of the following relationships will most help a privacy professional develop useful guidance for the organization?

- A. Relationships with individuals within the privacy professional community who are able to share expertise and leading practices for different industries.
- B. Relationships with clients, vendors, and customers whose data will be primarily collected and used throughout the organizational program.
- C. Relationships with company leaders responsible for approving, implementing, and periodically reviewing the corporate privacy program.
- D. Relationships with individuals across company departments and at different levels in the organization's hierarchy.

Correct Answer: C

[CIPP-US VCE Dumps](#)

[CIPP-US Practice Test](#)

[CIPP-US Braindumps](#)