CIPT$^{Q\&As}$

Certified Information Privacy Technologist (CIPT)

Pass IAPP CIPT Exam with 100% Guarantee

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

QUESTION 1

Which of the following would be the most appropriate solution for preventing privacy violations related to information exposure through an error message?

A. Configuring the environment to use shorter error messages.

B. Handing exceptions internally and not displaying errors to the user.

C. Creating default error pages or error messages which do not include variable data.

D. Logging the session name and necessary parameters once the error occurs to enable trouble shooting.

Correct Answer: C

QUESTION 2

SCENARIO

Looking back at your first two years as the Director of Personal Information Protection and Compliance for the St. Anne\\'s Regional Medical Center in Thorn Bay, Ontario, Canada, you see a parade of accomplishments, from developing state-of-the-art simulation based training for employees on privacy protection to establishing an interactive medical records system that is accessible by patients as well as by the medical personnel. Now, however, a question you have put off looms large: how do we manage all the data-not only records produced recently, but those still on-hand from years ago? A data flow diagram generated last year shows multiple servers, databases, and work stations, many of which hold files that have not yet been incorporated into the new records system. While most of this data is encrypted, its persistence may pose security and compliance concerns. The situation is further complicated by several long-term studies being conducted by the medical staff using patient information. Having recently reviewed the major Canadian privacy regulations, you want to make certain that the medical center is observing them.

You recall a recent visit to the Records Storage Section in the basement of the old hospital next to the modern facility, where you noticed paper records sitting in crates labeled by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. On the back shelves of the section sat data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the records storage section, you noticed a man leaving whom you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.

You quickly realize that you need a plan of action on the maintenance, secure storage and disposal of data.

Which cryptographic standard would be most appropriate for protecting patient credit card information in the records system at St. Anne\\'s Regional Medical Center?

A. Symmetric Encryption

B. Tokenization

C. Obfuscation

D. Certificates

Correct Answer: B

For protecting patient credit card information in the records system at St. Anne\\'s Regional Medical Center, tokenization is the most appropriate cryptographic standard. Tokenization involves replacing sensitive data elements, such as credit card numbers, with non-sensitive equivalents, referred to as tokens, which have no exploitable value. These tokens can then be used in the database and applications without bringing actual credit card details into the environment, thereby significantly reducing the risk of sensitive data breaches.

Tokenization is particularly effective for payment card data because it allows the system to function normally using tokens instead of real card numbers, ensuring that the data remains secure even if the system is compromised. This approach also helps in complying with payment card industry data security standards (PCI DSS), which strongly emphasize protecting cardholder data.

QUESTION 3

All of the following can be indications of a ransomware attack EXCEPT?

A. The inability to access certain files.

B. An increased amount of spam email in an individual\\'s inbox.

C. An increase in activity of the CPU of a computer for no apparent reason.

D. The detection of suspicious network communications between the ransomware and the attacker\\'s command and control servers.

Correct Answer: B

QUESTION 4

SCENARIO

Please use the following to answer the next question:

Light Blue Health (LBH) is a healthcare technology company developing a new web and mobile application that collects personal health information from electronic patient health records. The application will use machine learning to recommend potential medical treatments and medications based on information collected from anonymized electronic health records. Patient users may also share health data collected from other mobile apps with the LBH app.

The application requires consent from the patient before importing electronic health records into the application and sharing it with their authorized physicians or healthcare provider. The patient can then review and share the recommended treatments with their physicians securely through the app. The patient user may also share location data and upload photos in the app. The patient user may also share location data and upload photos in the app for a healthcare provider to review along with the health record. The patient may also delegate access to the app.

LBH\\'s privacy team meets with the Application development and Security teams, as well as key business stakeholders on a periodic basis. LBH also implements Privacy by Design (PbD) into the application development process.

The Privacy Team is conducting a Privacy Impact Assessment (PIA) to evaluate privacy risks during development of the application. The team must assess whether the application is collecting descriptive, demographic or any other user related data from the electronic health records that are not needed for the purposes of the application. The team is also reviewing whether the application may collect additional personal data for purposes for which the user did not provide consent.

The Privacy Team is conducting a Privacy Impact Assessment (PIA) for the new Light Blue Health application currently in development. Which of the following best describes a risk that is likely to result in a privacy breach?

A. Limiting access to the app to authorized personnel.

B. Including non-transparent policies, terms and conditions in the app.

C. Insufficiently deleting personal data after an account reaches its retention period.

D. Not encrypting the health record when it is transferred to the Light Blue Health servers.

Correct Answer: D

Not encrypting health records when they are transferred to Light Blue Health servers can leave sensitive personal information vulnerable to interception and unauthorized access. This could result in a privacy breach if an attacker were able to access this unencrypted data.

QUESTION 5

Which of the following is a privacy consideration for NOT sending large-scale SPAM type emails to a database of email addresses?

A. Poor user experience.

B. Emails are unsolicited.

C. Data breach notification.

D. Reduction in email deliverability score.

Correct Answer: B

Sending large-scale SPAM type emails involves dispatching bulk communications that recipients have not agreed to receive. This is a critical privacy consideration because unsolicited emails infringe on the privacy of individuals by using their personal information (such as email addresses) without consent. Such practices can violate privacy laws and regulations that require explicit permission for marketing communications, emphasizing the importance of obtaining consent prior to sending emails. This consent is central to respecting user privacy and complying with legal standards.