Vendor:IAPP

Exam Code:CIPT

Exam Name: Certified Information Privacy Technologist (CIPT)

Version: Demo

QUESTION 1

An organization needs to be able to manipulate highly sensitive personal information without revealing the contents of the data to the users. The organization should investigate the use of?

A. Advanced Encryption Standard (AES)

B. Homomorphic encryption

C. Quantum encryption

D. Pseudonymization

Correct Answer: B

if an organization needs to be able to manipulate highly sensitive personal information without revealing the contents of the data to the users, they should investigate the use of homomorphic encryption. Homomorphic encryption allows computations to be performed on encrypted data without revealing its contents.

QUESTION 2

Which of the following methods does NOT contribute to keeping the data confidential?

A. Differential privacy.

B. Homomorphic encryption.

C. K-anonymity.

D. Referential integrity.

Correct Answer: D

referential integrity does not contribute to keeping the data confidential.

QUESTION 3

Granting data subjects the right to have data corrected, amended, or deleted describes?

A. Use limitation.

B. Accountability.

C. A security safeguard

D. Individual participation

Correct Answer: D

Reference: https://www.ncbi.nlm.nih.gov/books/NBK236546/

Granting data subjects the right to have data corrected, amended, or deleted describes individual participation1. As explained above, the individual participation principle gives individuals certain rights over their personal data held by a data controller1. One of these rights is to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended1. The other options are not principles that describe granting data subjects this right.

QUESTION 4

How does browser fingerprinting compromise privacy?

A. By creating a security vulnerability.

B. By differentiating users based upon parameters.

C. By persuading users to provide personal information.

D. By customizing advertising based on the geographic location.

Correct Answer: B

browser fingerprinting compromises privacy by differentiating users based upon parameters. Browser fingerprinting involves collecting information about a user\\'s device and browser configuration in order to uniquely identify them. This can allow for tracking of user behavior across websites without their knowledge or consent.

QUESTION 5

What term describes two re-identifiable data sets that both come from the same unidentified individual?

A. Pseudonymous data.

B. Anonymous data.

C. Aggregated data.

D. Imprecise data.

Correct Answer: B

Reference: https://ico.org.uk/media/1061/anonymisation-code.pdf

---

QUESTION 6

Value sensitive design focuses on which of the following?

A. Quality and benefit.

B. Ethics and morality.

C. Confidentiality and integrity.

D. Consent and human rights.

Correct Answer: B

Value sensitive design (VSD) is a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner1. It brings human values to the forefront of the technical design process2.

QUESTION 7

Which privacy engineering objective proposed by the US National Institute of Science and Technology (NIST) decreases privacy risk by ensuring that connections between individuals and their personal data are reduced?

A. Disassoc lability

B. Manageability

C. Minimization

D. Predictability

Correct Answer: A

disassociability is a privacy engineering objective proposed by the US National Institute of Science and Technology (NIST) that decreases privacy risk by ensuring that connections between individuals and their personal data are reduced.

QUESTION 8

Which of the following suggests the greatest degree of transparency?

A. A privacy disclosure statement clearly articulates general purposes for collection

B. The data subject has multiple opportunities to opt-out after collection has occurred.

C. A privacy notice accommodates broadly defined future collections for new products.

D. After reading the privacy notice, a data subject confidently infers how her information will be used.

Correct Answer: D

After reading the privacy notice, a data subject confidently infers how her information will be used suggests the greatest degree of transparency3 https://www.informatica.com/resources/articles/what-is-data-quality.html

---

QUESTION 9

Which of the following is the best method to minimize tracking through the use of cookies?

A. Use `private browsing\\' mode and delete checked files, clear cookies and cache once a day.

B. Install a commercially available third-party application on top of the browser that is already installed.

C. Install and use a web browser that is advertised as `built specifically to safeguard user privacy\\'.

D. Manage settings in the browser to limit the use of cookies and remove them once the session completes.

Correct Answer: D

QUESTION 10

Not updating software for a system that processes human resources data with the latest security patches may create what?

A. Authentication issues.

B. Privacy vulnerabilities.

C. Privacy threat vectors.

D. Reportable privacy violations.

Correct Answer: B

QUESTION 11

During a transport layer security (TLS) session, what happens immediately after the web browser creates a random PreMasterSecret?

A. The server decrypts the PremasterSecret.

B. The web browser opens a TLS connection to the PremasterSecret.

C. The web browser encrypts the PremasterSecret with the server\\'s public key.

D. The server and client use the same algorithm to convert the PremasterSecret into an encryption key.

Correct Answer: C

Reference: https://books.google.com.pk/books?id=OaXise4B-p8Candpg=PA175andlpg=PA175anddq=iapp+During+a+transport+layer+security+(TLS)+session,+what+happens+immediately+after+the+web+browser+creates+a+random +PreMasterSecretandsource=blandots=zR0RCfnx3candsig=ACfU3U0bTOeOfPfcoq_Y95SZs6imKKilugandhl=enandsa=Xandved=2ahUKEwjkscDHpcbnAhUJuRoKHU5iC9cQ6AEwCnoECAkQAQ#v=onepageandq=iapp%20During%20a%20transport% 20layer%20security%20(TLS)%20session%2C%20what%20happens%20immediately%20after%20the%20web%20browser%20creates%20a%20random%20PreMasterSecretandf=false

---

QUESTION 12

A healthcare provider would like to data mine information for research purposes however the Chief Privacy Officer is concerned medical data of individuals may be disclosed overcome the concern, which is the preferred technique for protecting such data while still allowing for analysis?

A. Access Control

B. Encryption

C. Isolation

D. Perturbation

Correct Answer: D

perturbation would be a preferred technique for protecting medical data while still allowing for analysis. Perturbation involves adding noise or randomness to data in order to preserve privacy while still allowing for statistical analysis.