

IAPP

Exam Questions CIPT

Certified Information Privacy Technologist



NEW QUESTION 1

What is the main reason a company relies on implied consent instead of explicit consent from a user to process her data?

- A. The implied consent model provides the user with more detailed data collection information.
- B. To secure explicit consent, a user's website browsing would be significantly disrupted.
- C. An explicit consent model is more expensive to implement.
- D. Regulators prefer the implied consent model.

Answer: A

NEW QUESTION 2

Properly configured databases and well-written website codes are the best protection against what online threat?

- A. Pharming.
- B. SQL injection.
- C. Malware execution.
- D. System modification.

Answer: B

NEW QUESTION 3

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.

What is the best way to minimize the risk of an exposure violation through the use of the app?

- A. Prevent the downloading of photos stored in the app.
- B. Dissociate the patient health data from the personal data.
- C. Exclude the collection of personal information from the health record.
- D. Create a policy to prevent combining data with external data sources.

Answer: D

NEW QUESTION 4

What was the first privacy framework to be developed?

- A. OECD Privacy Principles.
- B. Generally Accepted Privacy Principles.
- C. Code of Fair Information Practice Principles (FIPPs).
- D. The Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

Answer: A

NEW QUESTION 5

A privacy engineer reviews a newly developed on-line registration page on a company's website. The purpose of the page is to enable corporate customers to submit a returns / refund request for physical goods. The page displays the following data capture fields: company name, account reference, company address, contact name, email address, contact phone number, product name, quantity, issue description and company bank account details.

After her review, the privacy engineer recommends setting certain capture fields as "non-mandatory". Setting which of the following fields as "non-mandatory" would be the best example of the principle of data minimization?

- A. The contact phone number field.
- B. The company address and name.
- C. The contact name and email address.
- D. The company bank account detail field.

Answer: B

NEW QUESTION 6

SCENARIO

WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider Azure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.

The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of Azure's privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing services provided by WebTracker, you will not be evaluating any internal data processing

activity, such as HR or Payroll.

This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome — a partnership that will not require any data sharing. SmartHome is based in the USA, and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.

To get an idea of the scope of work involved, you have decided to start reviewing the company's documentation and interviewing key staff to understand potential privacy risks.

The results of this initial work include the following notes:

- There are several typos in the current privacy notice of WebTracker, and you were not able to find the privacy notice for SmartHome.
- You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with AmaZure, which is responsible for the support and maintenance of the cloud infrastructure.
- There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.
- Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.
- All the WebTracker and SmartHome customers are based in USA and Canada.

Based on the initial assessment and review of the available data flows, which of the following would be the most important privacy risk you should investigate first?

- A. Verify that WebTracker's HR and Payroll systems implement the current privacy notice (after the typos are fixed).
- B. Review the list of subcontractors employed by AmaZure and ensure these are included in the formal agreement with WebTracker.
- C. Evaluate and review the basis for processing employees' personal data in the context of the prototype created by WebTracker and approved by the CEO.
- D. Confirm whether the data transfer from London to the USA has been fully approved by AmaZure and the appropriate institutions in the USA and the European Union.

Answer: C

NEW QUESTION 7

What is the main reason the Do Not Track (DNT) header is not acknowledged by more companies?

- A. Most web browsers incorporate the DNT feature.
- B. The financial penalties for violating DNT guidelines are too high.
- C. There is a lack of consensus about what the DNT header should mean.
- D. It has been difficult to solve the technological challenges surrounding DNT.

Answer: C

NEW QUESTION 8

How should the sharing of information within an organization be documented?

- A. With a binding contract.
- B. With a data flow diagram.
- C. With a disclosure statement.
- D. With a memorandum of agreement.

Answer: C

NEW QUESTION 9

What is typically NOT performed by sophisticated Access Management (AM) techniques?

- A. Restricting access to data based on location.
- B. Restricting access to data based on user role.
- C. Preventing certain types of devices from accessing data.
- D. Preventing data from being placed in unprotected storage.

Answer: B

NEW QUESTION 10

Which of these actions is NOT generally part of the responsibility of an IT or software engineer?

- A. Providing feedback on privacy policies.
- B. Implementing multi-factor authentication.
- C. Certifying compliance with security and privacy law.
- D. Building privacy controls into the organization's IT systems or software.

Answer: A

NEW QUESTION 11

Which of the following functionalities can meet some of the General Data Protection Regulation's (GDPR's) Data Portability requirements for a social networking app designed for users in the EU?

- A. Allow users to modify the data they provided the app.
- B. Allow users to delete the content they provided the app.
- C. Allow users to download the content they have provided the app.
- D. Allow users to get a time-stamped list of what they have provided the app.

Answer: C

NEW QUESTION 12

SCENARIO

Carol was a U.S.-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.

As business grew, Carol couldn't keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, "I don't know what you are doing, but keep doing it!" But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane's first impressions.

At the meeting, Carol could not wait to hear Jane's thoughts, but she was unprepared for what Jane had to say. "Carol, I know that he doesn't realize it, but some of Sam's efforts to increase sales have put you in a vulnerable position. You are not protecting customers' personal information like you should."

Sam said, "I am protecting our information. I keep it in the safe with our bank deposit. It's only a list of customers' names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That's the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase."

Carol replied, "Jane, that doesn't sound so bad. Could you just fix things and help us to post even more online?"

"I can," said Jane. "But it's not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy."

Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of the year, Carol shared some exciting news. "Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out! And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand."

What type of principles would be the best guide for Jane's ideas regarding a new data management program?

- A. Collection limitation principles.
- B. Vendor management principles.
- C. Incident preparedness principles.
- D. Fair Information Practice Principles

Answer: D

NEW QUESTION 13

Which of the following CANNOT be effectively determined during a code audit?

- A. Whether access control logic is recommended in all cases.
- B. Whether data is being incorrectly shared with a third-party.
- C. Whether consent is durably recorded in the case of a server crash.
- D. Whether the differential privacy implementation correctly anonymizes data.

Answer: D

NEW QUESTION 14

What is the term for information provided to a social network by a member?

- A. Profile data.
- B. Declared data.
- C. Personal choice data.
- D. Identifier information.

Answer: A

NEW QUESTION 15

Users of a web-based email service have their accounts breached through compromised login credentials. Which possible consequences of the breach illustrate the two categories of Calo's Harm Dimensions?

- A. Financial loss and blackmail.
- B. Financial loss and solicitation.
- C. Identity theft and embarrassment.
- D. Identity theft and the leaking of information.

Answer: D

NEW QUESTION 16

Which of the following is the least effective privacy preserving practice in the Systems Development Life Cycle (SDLC)?

- A. Conducting privacy threat modeling for the use-case.
- B. Following secure and privacy coding standards in the development.
- C. Developing data flow modeling to identify sources and destinations of sensitive data.
- D. Reviewing the code against Open Web Application Security Project (OWASP) Top 10 Security Risks.

Answer: C

NEW QUESTION 17

SCENARIO

Please use the following to answer the next question:

Chuck, a compliance auditor for a consulting firm focusing on healthcare clients, was required to travel to the client's office to perform an onsite review of the client's operations. He rented a car from Finley Motors upon arrival at the airport as so he could commute to and from the client's office. The car rental agreement was electronically signed by Chuck and included his name, address, driver's license, make/model of the car, billing rate, and additional details describing the rental transaction. On the second night, Chuck was caught by a red light camera not stopping at an intersection on his way to dinner. Chuck returned the car back to the car rental agency at the end week without mentioning the infraction and Finley Motors emailed a copy of the final receipt to the address on file.

Local law enforcement later reviewed the red light camera footage. As Finley Motors is the registered owner of the car, a notice was sent to them indicating the infraction and fine incurred. This notice included the license plate number, occurrence date and time, a photograph of the driver, and a web portal link to a video clip of the violation for further review. Finley Motors, however, was not responsible for the violation as they were not driving the car at the time and transferred the incident to AMP Payment Resources for further review. AMP Payment Resources identified Chuck as the driver based on the rental agreement he signed when picking up the car and then contacted Chuck directly through a written letter regarding the infraction to collect the fine.

After reviewing the incident through the AMP Payment Resources' web portal, Chuck paid the fine using his personal credit card. Two weeks later, Finley Motors sent Chuck an email promotion offering 10% off a future rental.

What should Finley Motors have done to incorporate the transparency principle of Privacy by Design (PbD)?

- A. Signed a data sharing agreement with AMP Payment Resources.
- B. Documented that Finley Motors has a legitimate interest to share Chuck's information.
- C. Obtained verbal consent from Chuck and recorded it within internal systems.
- D. Provided notice of data sharing practices within the electronically signed rental agreement.

Answer: D

NEW QUESTION 18

SCENARIO

Please use the following to answer next question:

EnsureClaim is developing a mobile app platform for managing data used for assessing car accident insurance claims. Individuals use the app to take pictures at the crash site, eliminating the need for a built-in vehicle camera. EnsureClaim uses a third-party hosting provider to store data collected by the app. EnsureClaim customer service employees also receive and review app data before sharing with insurance claim adjusters.

The app collects the following information: First and last name

Date of birth (DOB) Mailing address Email address

Car VIN number Car model License plate

Insurance card number Photo

Vehicle diagnostics Geolocation

What would be the best way to supervise the third-party systems the EnsureClaim App will share data with?

- A. Review the privacy notices for each third-party that the app will share personal data with to determine adequate privacy and data protection controls are in place.
- B. Conduct a security and privacy review before onboarding new vendors that collect personal data from the app.
- C. Anonymize all personal data collected by the app before sharing any data with third-parties.
- D. Develop policies and procedures that outline how data is shared with third-party apps.

Answer: C

NEW QUESTION 19

After committing to a Privacy by Design program, which activity should take place first?

- A. Create a privacy standard that applies to all projects and services.
- B. Establish a retention policy for all data being collected.
- C. Implement easy to use privacy settings for users.
- D. Perform privacy reviews on new projects.

Answer: B

NEW QUESTION 20

Which of the following does NOT illustrate the 'respect to user privacy' principle?

- A. Implementing privacy elements within the user interface that facilitate the use of technology by any visually-challenged users.
- B. Enabling Data Subject Access Request (DSARs) that provide rights for correction, deletion, amendment and rectification of personal information.
- C. Developing a consent management self-service portal that enables the data subjects to review the details of consent provided to an organization.
- D. Filing breach notification paperwork with data protection authorities which detail the impact to data subjects.

Answer: D

NEW QUESTION 21

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CIPT Practice Exam Features:

- * CIPT Questions and Answers Updated Frequently
- * CIPT Practice Questions Verified by Expert Senior Certified Staff
- * CIPT Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CIPT Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CIPT Practice Test Here](#)