CIPT Q&As

Certified Information Privacy Technologist (CIPT)

Pass IAPP CIPT Exam with 100% Guarantee

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

https://www.pass2lead.com/cipt.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

What is a main benefit of data aggregation?

A. It is a good way to perform analysis without needing a statistician.

B. It applies two or more layers of protection to a single data record.

C. It allows one to draw valid conclusions from small data samples.

D. It is a good way to achieve de-identification and unlinkabilty.

Correct Answer: C

QUESTION 2

SCENARIO

Looking back at your first two years as the Director of Personal Information Protection and Compliance for the Berry Country 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 also recall a recent visit to the Records Storage Section, often termed "The Dungeon" in the basement of the old hospital next to the modern facility, where you noticed a multitude of paper records. Some of these were in crates marked by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. The back shelves of the section housed data tapes and old hard drives that were often unlabeled but

appeared to be years old. On your way out of the dungeon, you noticed just ahead of you a small man in a lab coat who you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.

Which data lifecycle phase needs the most attention at this Ontario medical center?

A. Retention

B. Disclosure

C. Collection

D. Use

Correct Answer: A

QUESTION 3

An organization is concerned that its aging IT infrastructure will lead to Increased security and privacy risks. Which of the following would help mitigate these risks?

A. Vulnerability management.

B. Data Loss Prevention.

C. Code audits.

D. Network Centricity.

Correct Answer: A

vulnerability management would help mitigate the risks of an organization\\'s aging IT infrastructure leading to increased security and privacy risks.

QUESTION 4

A credit card with the last few numbers visible is an example of what?

A. Masking data

B. Synthetic data

C. Sighting controls.

D. Partial encryption

Correct Answer: A

Reference: https://money.stackexchange.com/questions/98951/credit-card-number-masking-good-practices-rules-law-regulations

QUESTION 5

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 6

Machine-learning based solutions present a privacy risk because?

A. Training data used during the training phase is compromised.

B. The solution may contain inherent bias from the developers.

C. The decision-making process used by the solution is not documented.

D. Machine-learning solutions introduce more vulnerabilities than other software.

Correct Answer: B

machine-learning based solutions present a privacy risk because they may contain inherent bias from the developers. Bias can be introduced into machine learning models through biased training data or through biased decision-making processes used by the solution.

QUESTION 7

In order to prevent others from identifying an individual within a data set, privacy engineers use a cryptographically-secure hashing algorithm. Use of hashes in this way illustrates the privacy tactic known as what?

A. Isolation.

B. Obfuscation.

C. Perturbation.

D. Stripping.

Correct Answer: B

QUESTION 8

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

Correct Answer: D

Reference: https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair- information-practices/

QUESTION 9

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

a privacy consideration for NOT sending large-scale SPAM type emails to a database of email addresses is that the emails are unsolicited. Sending unsolicited emails can violate individuals\\' privacy rights and may also be illegal under certain anti-spam laws.

QUESTION 10

SCENARIO

Please use the following to answer the next questions:

Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub. This is accessible through the \\'Settings\\' icon from any app page, then clicking \\'My Preferences\\', and selecting \\'Information Sharing and Consent\\' where the following choices are displayed:

1.

"I consent to receive notifications and infection alerts";

2.

"I consent to receive information on additional features or services, and new products";

3.

"I consent to sharing only my risk result and location information, for exposure and contact tracing purposes";

4.

"I consent to share my data for medical research purposes"; and

5.

"I consent to share my data with healthcare providers affiliated to the company".

For each choice, an ON* or OFF tab is available The default setting is ON for all

Users purchase a virus screening service for USS29 99 for themselves or others using the app The virus screening service works as follows:

1.

Step 1 A photo of the user\\'s face is taken.

2.

Step 2 The user measures their temperature and adds the reading in the app

3.

Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms

4.

Step 4 The user is asked to answer questions on known symptoms

5.

Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).)

The results are displayed as one of the following risk status "Low. "Medium" or "High" if the user is deemed at "Medium " or "High" risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic

from a healthcare provider.

A user\\'s risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as "medium\\' or \\'high\\' risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone\\'s GPS functionary, whether the app is in use or not however, the exact location of the user is "blurred\\' for privacy reasons Users can only see on the map circles

What is likely to be the biggest privacy concern with the current \\'Information Sharing and Consent\\' page?

A. The ON or OFF default setting for each item.

B. The navigation needed in the app to get to the consent page.

C. The option to consent to receive potential marketing information.

D. The information sharing with healthcare providers affiliated with the company.

Correct Answer: A

Having default settings for information sharing and consent can be problematic because it may not accurately reflect a user\\'s preferences. Users may not be aware of these default settings or may not understand their implications. This could result in personal information being shared without the user\\'s explicit consent.

QUESTION 11

A privacy technologist has been asked to aid in a forensic investigation on the darknet following the compromise of a company\\'s personal data. This will primarily involve an understanding of which of the following privacy-preserving techniques?

A. Encryption

B. Do Not Track

C. Masking

D. Tokenization

Correct Answer: A

a privacy technologist aiding in a forensic investigation on the darknet following the compromise of a company\\'s personal data would primarily need an understanding of encryption. Encryption is a privacy-preserving technique that can help protect sensitive data from unauthorized access.

QUESTION 12

SCENARIO

Please use the following to answer the next question:

Jordan just joined a fitness-tracker start-up based in California, USA, as its first Information Privacy and Security Officer. The company is quickly growing its business but does not sell any of the fitness trackers itself. Instead, it relies on a

distribution network of third-party retailers in all major countries. Despite not having any stores, the company has a 78% market share in the EU. It has a website presenting the company and products, and a member section where customers can access their information. Only the email address and physical address need to be provided as part of the registration process in order to customize the site to the user\\'s region and country. There is also a newsletter sent every month to all members featuring fitness tips, nutrition advice, product spotlights from partner companies based on user behavior and preferences.

Jordan says the General Data Protection Regulation (GDPR) does not apply to the company. He says the company is not established in the EU, nor does it have a processor in the region. Furthermore, it does not do any "offering goods or services" in the EU since it does not do any marketing there, nor sell to consumers directly. Jordan argues that it is the customers who chose to buy the products on their own initiative and there is no "offering" from the company.

The fitness trackers incorporate advanced features such as sleep tracking, GPS tracking, heart rate monitoring. wireless syncing, calorie-counting and step-tracking. The watch must be paired with either a smartphone or a computer in order to collect data on sleep levels, heart rates, etc. All information from the device must be sent to the company\\'s servers in order to be processed, and then the results are sent to the smartphone or computer. Jordan argues that there is no personal information involved since the company does not collect banking or social security information.

Why is Jordan\\'s claim that the company does not collect personal information as identified by the GDPR inaccurate?

A. The potential customers must browse for products online.

B. The fitness trackers capture sleep and heart rate data to monitor an individual\\'s behavior.

C. The website collects the customers\\' and users\\' region and country information.

D. The customers must pair their fitness trackers to either smartphones or computers.

Correct Answer: B

Sleep and heart rate data collected by the fitness trackers can be considered personal information under the GDPR because it relates to an identified or identifiable natural person. This means that even if the company does not collect other types of personal information such as name or address, it is still collecting personal information as defined by the GDPR.

QUESTION 13

What is an example of a just-in-time notice?

A. A warning that a website may be unsafe.

B. A full organizational privacy notice publicly available on a website

C. A credit card company calling a user to verify a purchase before itis authorized

D. Privacy information given to a user when he attempts to comment on an online article.

Correct Answer: D

Reference: https://www.clarip.com/data-privacy/just-time-notices/

QUESTION 14

An organization has recently experienced a data breach where large amounts of personal data were compromised. As part of a post-incident review, the privacy technologist wants to analyze available data to understand what vulnerabilities may have contributed to the incident occurring. He learns that a key vulnerability had been flagged by the system but that detective controls were not operating effectively. Which type of web application security risk does this finding most likely point to?

A. Insecure Design.

B. Misconfiguration.

C. Vulnerable and Outdated Components.

D. Logging and Monitoring Failures.

Correct Answer: D

if an organization has recently experienced a data breach where large amounts of personal data were compromised and a post-incident review reveals that a key vulnerability had been flagged by the system but that detective controls were not operating effectively, this finding most likely points to logging and monitoring failures as a type of web application security risk. Effective logging and monitoring can help detect and respond to security incidents in a timely manner.

QUESTION 15

What has been identified as a significant privacy concern with chatbots?

A. Most chatbot providers do not agree to code audits

B. Chatbots can easily verify the identity of the contact.

C. Users\\' conversations with chatbots are not encrypted in transit.

D. Chatbot technology providers may be able to read chatbot conversations with users.

Correct Answer: D

Reference: https://resources.infosecinstitute.com/privacy-concerns-emotional-chatbots/