

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

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

Answer: D

NEW QUESTION 4

SCENARIO

Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in-house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.

The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario. With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.

In a business strategy session held by senior management recently, Clean-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms.

The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

- A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
- A resource facing web interface that enables resources to apply and manage their assigned jobs.
- An online payment facility for customers to pay for services.

If Clean-Q were to utilize LeadOps' services, what is a contract clause that may be included in the agreement entered into with LeadOps?

- A. A provision that holds LeadOps liable for a data breach involving Clean-Q's information.
- B. A provision prescribing technical and organizational controls that LeadOps must implement.
- C. A provision that requires LeadOps to notify Clean-Q of any suspected breaches of information that involves customer or resource information managed on behalf of Clean-Q.
- D. A provision that allows Clean-Q to conduct audits of LeadOps' information processing and information security environment, at LeadOps' cost and at any time that Clean-Q requires.

Answer: D

NEW QUESTION 5

What is the main function of the Amnesic Incognito Live System or TAILS device?

- A. It allows the user to run a self-contained computer from a USB device.
- B. It accesses systems with a credential that leaves no discernable tracks.
- C. It encrypts data stored on any computer on a network.
- D. It causes a system to suspend its security protocols.

Answer: A

NEW QUESTION 6

Which is NOT a drawback to using a biometric recognition system?

- A. It can require more maintenance and support.
- B. It can be more expensive than other systems
- C. It has limited compatibility across systems.
- D. It is difficult for people to use.

Answer: A

NEW QUESTION 7

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 8

What tactic does pharming use to achieve its goal?

- A. It modifies the user's Hosts file.
- B. It encrypts files on a user's computer.
- C. It creates a false display advertisement.
- D. It generates a malicious instant message.

Answer: C

NEW QUESTION 9

Under the Family Educational Rights and Privacy Act (FERPA), releasing personally identifiable information from a student's educational record requires written permission from the parent or eligible student in order for information to be?

- A. Released to a prospective employer.
- B. Released to schools to which a student is transferring.
- C. Released to specific individuals for audit or evaluation purposes.
- D. Released in response to a judicial order or lawfully ordered subpoena.

Answer: C

NEW QUESTION 10

What is true of providers of wireless technology?

- A. They have the legal right in most countries to control and use any data on their systems.
- B. They can see all unencrypted data that crosses the system.
- C. They are typically exempt from data security regulations.
- D. They routinely backup data that crosses their system.

Answer: B

NEW QUESTION 10

What is the main privacy threat posed by Radio Frequency Identification (RFID)?

- A. An individual with an RFID receiver can track people or consumer products.
- B. An individual can scramble computer transmissions in weapons systems.
- C. An individual can use an RFID receiver to engage in video surveillance.
- D. An individual can tap mobile phone communications.

Answer: D

NEW QUESTION 11

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 16

What is the goal of privacy enhancing technologies (PETS) like multiparty computation and differential privacy?

- A. To facilitate audits of third party vendors.
- B. To protect sensitive data while maintaining its utility.
- C. To standardize privacy activities across organizational groups.
- D. To protect the security perimeter and the data items themselves.

Answer: B

NEW QUESTION 20

SCENARIO

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as "My Cool Ride" for automobile-related products or "Zoomer" for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third- party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as "Under the Sun." The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

Which should be used to allow the home sales force to accept payments using smartphones?

- A. Field transfer protocol.
- B. Cross-current translation.
- C. Near-field communication
- D. Radio Frequency Identification

Answer: C

NEW QUESTION 23

SCENARIO

Please use the following to answer the next question:

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

Answer: B

NEW QUESTION 27

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 unlinkability.

Answer: C

NEW QUESTION 31

What must be used in conjunction with disk encryption?

- A. Increased CPU speed.

- B. A strong password.
- C. A digital signature.
- D. Export controls.

Answer: C

NEW QUESTION 36

An organization based in California, USA is implementing a new online helpdesk solution for recording customer call information. The organization considers the capture of personal data on the online helpdesk solution to be in the interest of the company in best servicing customer calls. Before implementation, a privacy technologist should conduct which of the following?

- A. A Data Protection Impact Assessment (DPIA) and consultation with the appropriate regulator to ensure legal compliance.
- B. A privacy risk and impact assessment to evaluate potential risks from the proposed processing operations.
- C. A Legitimate Interest Assessment (LIA) to ensure that the processing is proportionate and does not override the privacy, rights and freedoms of the customers.
- D. A security assessment of the help desk solution and provider to assess if the technology was developed with a security by design approach.

Answer: C

NEW QUESTION 38

Value Sensitive Design (VSD) focuses on which of the following?

- A. Quality and benefit.
- B. Ethics and morality.
- C. Principles and standards.
- D. Privacy and human rights.

Answer: C

NEW QUESTION 40

What Privacy by Design (PbD) element should include a de-identification or deletion plan?

- A. Categorization.
- B. Remediation.
- C. Retention.
- D. Security

Answer: C

NEW QUESTION 43

What is the main benefit of using dummy data during software testing?

- A. The data comes in a format convenient for testing.
- B. Statistical disclosure controls are applied to the data.
- C. The data enables the suppression of particular values in a set.
- D. Developers do not need special privacy training to test the software.

Answer: D

NEW QUESTION 46

Which Organization for Economic Co-operation and Development (OECD) privacy protection principle encourages an organization to obtain an individual's consent before transferring personal information?

- A. Individual participation.
- B. Purpose specification.
- C. Collection limitation.
- D. Accountability.

Answer: C

NEW QUESTION 48

Which of the following entities would most likely be exempt from complying with the General Data Protection Regulation (GDPR)?

- A. A South American company that regularly collects European customers' personal data.
- B. A company that stores all customer data in Australia and is headquartered in a European Union (EU) member state.
- C. A Chinese company that has opened a satellite office in a European Union (EU) member state to service European customers.
- D. A North American company servicing customers in South Africa that uses a cloud storage system made by a European company.

Answer: C

NEW QUESTION 53

What distinguishes a "smart" device?

- A. It can perform multiple data functions simultaneously.
- B. It is programmable by a user without specialized training.
- C. It can reapply access controls stored in its internal memory.

D. It augments its intelligence with information from the internet.

Answer: D

NEW QUESTION 55

Organizations understand there are aggregation risks associated with the way the process their customer's data. They typically include the details of this aggregation risk in a privacy notice and ask that all customers acknowledge they understand these risks and consent to the processing. What type of risk response does this notice and consent represent?

- A. Risk transfer.
- B. Risk mitigation.
- C. Risk avoidance.
- D. Risk acceptance.

Answer: A

NEW QUESTION 59

Which technique is most likely to facilitate the deletion of every instance of data associated with a deleted user account from every data store held by an organization?

- A. Auditing the code which deletes user accounts.
- B. Building a standardized and documented retention program for user data deletion.
- C. Monitoring each data store for presence of data associated with the deleted user account.
- D. Training engineering teams on the importance of deleting user accounts their associated data from all data stores when requested.

Answer: C

NEW QUESTION 64

Which is NOT a way to validate a person's identity?

- A. Swiping a smartcard into an electronic reader.
- B. Using a program that creates random passwords.
- C. Answering a question about "something you know".
- D. Selecting a picture and tracing a unique pattern on it

Answer: B

NEW QUESTION 66

SCENARIO

It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card. You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain

Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.

"We were hacked twice last year," Dr. Batch says, "and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again." She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.

You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?

You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key.

Still pondering, you attempt to pull up the facility's

wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.

What type of wireless network does GFDC seem to employ?

- A. A hidden network.
- B. A reluctant network.
- C. A user verified network.
- D. A wireless mesh network.

Answer: A

NEW QUESTION 67

What would be an example of an organization transferring the risks associated with a data breach?

- A. Using a third-party service to process credit card transactions.
- B. Encrypting sensitive personal data during collection and storage
- C. Purchasing insurance to cover the organization in case of a breach.
- D. Applying industry standard data handling practices to the organization' practices.

Answer: C

NEW QUESTION 71

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.

Answer: A

NEW QUESTION 72

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 75

SCENARIO

It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card. You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain

Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.

"We were hacked twice last year," Dr. Batch says, "and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again." She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.

You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?

You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility's wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.

Why would you recommend that GFC use record encryption rather than disk, file or table encryption?

- A. Record encryption is asymmetric, a stronger control measure.
- B. Record encryption is granular, limiting the damage of potential breaches.
- C. Record encryption involves tag masking, so its metadata cannot be decrypted
- D. Record encryption allows for encryption of personal data only.

Answer: B

NEW QUESTION 80

SCENARIO

Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in-house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.

The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.

With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings. In a business strategy session held by senior management recently, Clean-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms. The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution on a single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

- A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
- A resource facing web interface that enables resources to apply and manage their assigned jobs.
- An online payment facility for customers to pay for services.

What is a key consideration for assessing external service providers like LeadOps, which will conduct personal information processing operations on Clean-Q's behalf?

- A. Understanding LeadOps' costing model.
- B. Establishing a relationship with the Managing Director of LeadOps.
- C. Recognizing the value of LeadOps' website holding a verified security certificate.
- D. Obtaining knowledge of LeadOps' information handling practices and information security environment.

Answer: D

NEW QUESTION 84

Which of the following is considered a client-side IT risk?

- A. Security policies focus solely on internal corporate obligations.
- B. An organization increases the number of applications on its server.
- C. An employee stores his personal information on his company laptop.
- D. IDs used to avoid the use of personal data map to personal data in another database.

Answer: C

NEW QUESTION 87

A company seeking to hire engineers in Silicon Valley ran an ad campaign targeting women in a specific age range who live in the San Francisco Bay Area. Which Calo objective privacy harm is likely to result from this campaign?

- A. Lost opportunity.
- B. Economic loss.
- C. Loss of liberty.
- D. Social detriment.

Answer: D

NEW QUESTION 90

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 92

A privacy engineer has been asked to review an online account login page. He finds there is no limitation on the number of invalid login attempts a user can make when logging into their online account.

What would be the best recommendation to minimize the potential privacy risk from this weakness?

- A. Implement a CAPTCHA system.
- B. Develop server-side input validation checks.
- C. Enforce strong password and account credentials.
- D. Implement strong Transport Layer Security (TLS) to ensure an encrypted link.

Answer: B

NEW QUESTION 95

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 100

Which of the following would be the best method of ensuring that Information Technology projects follow Privacy by Design (PbD) principles?

- A. Develop a technical privacy framework that integrates with the development lifecycle.
- B. Utilize Privacy Enhancing Technologies (PETs) as a part of product risk assessment and management.
- C. Identify the privacy requirements as a part of the Privacy Impact Assessment (PIA) process during development and evaluation stages.
- D. Develop training programs that aid the developers in understanding how to turn privacy requirements into actionable code and design level specifications.

Answer: D

NEW QUESTION 103

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 107

Aadhaar is a unique-identity number of 12 digits issued to all Indian residents based on their biometric and demographic data. The data is collected by the Unique Identification Authority of India. The Aadhaar database contains the Aadhaar number, name, date of birth, gender and address of over 1 billion individuals.

Which of the following datasets derived from that data would be considered the most de-identified?

- A. A count of the years of birth and hash of the person's gender.
- B. A count of the month of birth and hash of the person's first name.
- C. A count of the day of birth and hash of the person's first initial of their first name.
- D. Account of the century of birth and hash of the last 3 digits of the person's Aadhaar number.

Answer: C

NEW QUESTION 108

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.

Answer: D

NEW QUESTION 112

A company configures their information system to have the following capabilities: Allow for selective disclosure of attributes to certain parties, but not to others.

Permit the sharing of attribute references instead of attribute values - such as "I am over 21" instead of birthday date.

Allow for information to be altered or deleted as needed.

These capabilities help to achieve which privacy engineering objective?

- A. Predictability.
- B. Manageability.
- C. Disassociability.
- D. Integrity.

Answer: C

NEW QUESTION 116

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 121

SCENARIO

Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company's information

security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle's schedule included participating in meetings and observing work in the IT and compliance departments.

Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization's wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.

Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company's privacy risk assessment, noting that the secondary use of personal information was considered a high risk.

By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.

Ted's implementation is most likely a response to what incident?

- A. Encryption keys were previously unavailable to the organization's cloud storage host.
- B. Signatureless advanced malware was detected at multiple points on the organization's networks.
- C. Cyber criminals accessed proprietary data by running automated authentication attacks on the organization's network.
- D. Confidential information discussed during a strategic teleconference was intercepted by the organization's top competitor.

Answer: A

NEW QUESTION 126

.....

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](#)