PassQueen
a.k.a dumpsqueen.com

Certified Information Privacy Technologist (CIPT)

IAPP CIPT

Version Demo

Total Demo Questions: 30

Total Premium Questions: 309

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Foundational Principles	66
Topic 2, The Role of the Privacy Technologist	10
Topic 3, Privacy Risks	73
Topic 4, Technical Measures and Privacy-Enhancing Technologies	114
Topic 5, Privacy by Design Methodology	28
Topic 6, Privacy in the Engineering Lifecycle	18
Total	309

QUESTION NO: 1

Which of the following provides a mechanism that allows an end-user to use a single sign-on (SSO) for multiple services?

A. The OpenID Federation.

B. PCI Data Security Standards Council

C. International Organization for Standardization.

D. Personal Information Protection and Electronic Documents Act.

ANSWER: A

Explanation:

The OpenID Federation provides a trust framework that can support single sign-on across multiple services. In a federated identity model, a user authenticates with an identity provider that is trusted by the services they want to access, rather than creating and managing separate credentials for each service. The identity provider issues signed identity assertions or tokens, and relying services validate those assertions based on established federation metadata and trust relationships. This allows authentication to be centralized while still permitting multiple independent service providers to make their own authorization decisions about the authenticated user.

OpenID Federation is designed to describe and distribute the metadata, keys, policies, and trust chains that participants use to establish those relationships at scale. It complements OpenID Connect, whose core specification defines an interoperable identity layer using OAuth-based flows and ID Tokens. In practical terms, this architecture reduces password reuse and credential proliferation, supports consistent authentication controls, and gives users a smoother sign-in experience across participating services. The OpenID Foundation's OpenID Federation specification describes this trust model, while the OpenID Connect Core specification explains the identity and authentication protocol commonly used with it.

QUESTION NO: 2 - (SIMULATION)

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 regulation most likely applies to the data stored by Berry Country Regional Medical Center?

ANSWER: See the explanation for the answer

Explanation:

Answer: PIPEDA (the Personal Information Protection and Electronic Documents Act).

The medical center is in Ontario, Canada, and holds identifiable patient and employee-related information. Of the listed choices, PIPEDA is the applicable Canadian federal private-sector privacy law. HIPAA applies in the United States, the Health Records Act 2001 is a Victorian (Australia) law, and EU Directive 95/46/EC was European legislation.

In practice, Ontario health-information custodians are principally subject to Ontario's **Personal Health Information Protection Act, 2004 (PHIPA)**, which is substantially similar to PIPEDA and generally overrides PIPEDA for regulated personal health information activities. However, because PHIPA is not an answer option, select **PIPEDA**.

Reference: Personal Information Protection and Electronic Documents Act (PIPEDA)

QUESTION NO: 3

Which of the following can be used to bypass even the best physical and logical security mechanisms to gain access to a system?

A. Phishing emails.

B. Denial of service.

C. Brute-force attacks.

D. Social engineering.

ANSWER: D

Explanation:

Social engineering is correct because it targets the human element of security rather than attempting to defeat a technical control directly. An attacker may manipulate an employee, contractor, administrator, or other trusted individual into disclosing credentials, approving a request, granting physical entry, installing software, or performing another action that creates unauthorized access. This can circumvent carefully designed physical safeguards, such as badges and locked areas, as well as logical safeguards, such as authentication controls, network segmentation, and access permissions, because the authorized person is induced to act on the attacker's behalf.

For privacy technologists, this illustrates why effective security and privacy programs must combine technical controls with organizational measures: clear procedures, verification practices, role-appropriate training, reporting channels, and a culture in which unusual requests can be challenged. The U.S. Cybersecurity and Infrastructure Security Agency describes social engineering as techniques used to manipulate people into taking actions or divulging confidential information, emphasizing the risk posed by human manipulation. NIST likewise recognizes social engineering as an attack approach centered on exploiting human trust and behavior. See CISA's guidance on social engineering and phishing and NIST's Social Engineering glossary entry.

QUESTION NO: 4

A product team is adding a feature that uses precise location information to recommend nearby services.

Which design choices would best implement privacy by default?

A. Collect precise location only when the nearby-services feature is invoked.

B. Set location sharing to off until the user makes an affirmative choice.

C. Enable continuous background location collection for all users.

D. Combine location permission with consent to marketing communications.

ANSWER: A B

Explanation:

Collecting precise location only when a user actively invokes the nearby-services feature limits processing to the context in which location is needed. It avoids continuous background collection that would create a broader record of the user's movements without being necessary for the requested service.

Setting location sharing to off until the user makes an affirmative choice also implements a privacy-protective default. The product should provide understandable contextual information when location access is requested, including why it is needed and how long it will be used or retained. Privacy by default seeks to ensure that the least privacy-invasive settings operate unless an individual chooses otherwise. The ICO explains this approach in its guidance on data protection by design and default.

QUESTION NO: 5

A company plans to deploy a machine-learning model that predicts whether applicants are likely to qualify for a financial product.

Which practices would best help manage privacy and fairness risks throughout the model lifecycle?

A. Evaluate training data for representativeness and potential bias.

B. Document model features, data sources and limitations.

C. Monitor outcomes after deployment for unexpected impacts.

D. Remove human oversight after the model is approved.

ANSWER: A B C

Explanation:

Evaluating training data for representativeness and potential bias can help identify whether the data may produce systematically unfair results for particular groups. Documenting features, training sources, performance measures and known limitations supports transparency, accountability and later investigation. Monitoring deployed outcomes is also necessary because model performance and impacts can change as data, populations and operating conditions change.

Removing all human oversight would not manage these risks. Appropriate governance should define accountability, review processes and escalation paths for problematic outcomes. The NIST AI Risk Management Framework emphasizes governance, measurement and ongoing management of AI risks.

QUESTION NO: 6

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.

ANSWER: B

Explanation:

Privacy vulnerabilities. Security patches remediate known software flaws that attackers could otherwise exploit. When an organization fails to apply relevant patches to a system handling human resources data, the unremediated flaws can permit unauthorized access, disclosure, alteration, or loss of personal information such as employee identifiers, compensation information, performance records, or benefits data. This creates a privacy vulnerability because a weakness in the technology or its configuration can undermine the confidentiality, integrity, and availability protections needed for personal data.

In privacy engineering, technical security weaknesses matter because they may enable a privacy-impacting event even before an exploit or disclosure has occurred. Patch management is therefore a core preventative control: organizations need processes to identify applicable updates, assess and prioritize their risk, test where appropriate, deploy them promptly, and verify successful installation. NIST's guidance describes enterprise patch management as a process for identifying, acquiring, installing, and verifying patches to reduce exposure to vulnerabilities. The UK National Cyber Security Centre likewise emphasizes that applying updates is an important means of fixing security weaknesses. See NIST SP 800-40 Rev. 4 and NCSC guidance on applying updates.

QUESTION NO: 7

A user who owns a resource wants to give other individuals access to the resource. What control would apply?

A. Mandatory access control.

B. Role-based access controls.

C. Discretionary access control.

D. Context of authority controls.

ANSWER: C

Explanation:

Discretionary access control is the appropriate control because it gives the owner or creator of a resource the discretion to determine who may access it and what permissions they receive. The resource owner can grant, modify, or revoke access for individual users, typically by maintaining an access-control list or setting permissions on the resource. This model directly supports the situation described: an individual who owns a resource independently chooses to share it with others.

In practice, discretionary access control is common in operating systems and file-sharing environments. For example, a file owner may assign read, write, or execute permissions to specified users or groups. The defining feature is that access decisions are delegated to the resource owner rather than being imposed exclusively by a centrally defined security classification or organizational policy. This owner-controlled delegation makes discretionary access control especially useful where users need flexibility to collaborate and share resources they create or manage.

For further background, see the NIST definition of discretionary access control and the OWASP Authorization Cheat Sheet.

QUESTION NO: 8

Which of the following statements is true regarding software notifications and agreements?

A. Website visitors must view the site's privacy statement before downloading software.

B. Software agreements are designed to be brief, while notifications provide more details.

C. It is a good practice to provide users with information about privacy prior to software installation.

D. "Just in time" software agreement notifications provide users with a final opportunity to modify the agreement.

ANSWER: C

Explanation:

It is a good practice to provide users with information about privacy prior to software installation. Providing meaningful notice before installation gives individuals an opportunity to understand what personal data the software may collect, use, disclose, or transmit; the purposes for those activities; and any relevant choices or controls available to them. This timing supports transparency because users can make an informed decision before the software begins operating or collecting data. Notice should be presented in a clear, conspicuous, and accessible manner, rather than being deferred until after installation, when data processing may already have started. Where the installation involves optional data practices, privacy-by-design principles also support offering appropriate controls at that decision point. The U.S. Federal Trade Commission's guidance on privacy by design emphasizes transparency and providing consumers with appropriate notice and choice, particularly for

uses of data that may not be expected in context. The NIST Privacy Framework likewise identifies communication with individuals and providing meaningful privacy information as key elements of privacy risk management. See the FTC privacy recommendations and the NIST Privacy Framework.

QUESTION NO: 9

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:

• "I consent to receive notifications and infection alerts";

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

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

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

• "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:

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

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

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

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

• 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

Which of the following is likely to be the most important issue with the choices presented in the 'Information Sharing and Consent' pages?

A. The data and recipients for medical research are not specified

B. Insufficient information is provided on notifications and infection alerts

C. The sharing of information with an affiliated healthcare provider is too risky

D. Allowing users to share risk result information for exposure and contact tracing purposes

ANSWER: A B

Explanation:

Meaningful consent depends on a person receiving clear, understandable information about the processing before making a choice. “The data and recipients for medical research are not specified” is therefore a central defect: medical research can involve sensitive health, biometric, location, and inferred risk information, yet the choice does not identify the categories of data involved, the research purpose, or the organizations that may receive or use it. A user cannot meaningfully assess the implications of that sharing from the wording provided.

“Insufficient information is provided on notifications and infection alerts” is also an important issue because these alerts may depend on processing or disclosing highly sensitive risk and proximity information. The consent text should clearly state what triggers an alert, what data is used or shared, who receives it, and whether the alert can reveal information about another person. Providing this context supports transparency and user control, particularly where the service concerns health and contact tracing. These requirements align with the FTC’s guidance that privacy notices should clearly describe data practices and with NIST’s privacy engineering approach of enabling predictability and manageability for individuals. See the FTC’s Mobile Privacy Disclosures guidance and NIST Privacy Framework.

QUESTION NO: 10

A company is beginning development of a mobile application that will collect account information, contacts and device location data.

Which activities should occur during the requirements phase to support privacy by design?

A. Document the intended purposes for each data element.

B. Identify the minimum data needed for each feature.

C. Define retention and deletion requirements.

D. Collect all available device data for future product uses.

ANSWER: A B C

Explanation:

Documenting the intended processing purposes and identifying the personal data necessary for each purpose are appropriate requirements-phase activities. These steps enable the team to assess whether each data element is relevant and proportionate before the application architecture and interfaces are established.

Defining retention and deletion requirements early is also appropriate. Retention is a lifecycle decision that affects database design, backup processes, vendor arrangements and automated disposition capabilities. Deferring these decisions until deployment can result in systems that retain personal information indefinitely because they lack a practical deletion mechanism.

Privacy engineering integrates privacy requirements into system-development activities so that data processing is predictable and manageable. See the NIST Privacy Framework and the UK ICO guidance on data protection by design and default.

QUESTION NO: 11

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."

When initially collecting personal information from customers, what should Jane be guided by?

A. Onward transfer rules.

B. Digital rights management.

C. Data minimization principles.

D. Vendor management principles

E. Purpose limitation principles.

ANSWER: C E

Explanation:

Jane should apply data minimization and purpose limitation at the point of collection. Data minimization requires the boutique to collect personal information that is adequate, relevant, and limited to what is necessary for a defined business need. For example, information necessary to process an online order, deliver a glass item, or respond to a customer inquiry may be appropriate, while collecting additional details merely because they might be useful later would not align with this principle.

Purpose limitation complements minimization by requiring Jane to identify and communicate the specific purpose before or when information is collected, then use the information consistently with that purpose. If the boutique intends to use contact details for marketing newly completed pieces, that intended use should be clearly described and managed separately from data collected solely to fulfill a purchase. Defining purposes up front also enables meaningful customer choices and supports later decisions about retention, access controls, vendor processing, and any proposed transfer during an acquisition.

These principles are reflected in the Fair Information Practice Principles and in the NIST Privacy Framework’s focus on data processing that is predictable, manageable, and appropriately governed. See the FTC’s privacy-framework guidance and the NIST Privacy Framework.

QUESTION NO: 12

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: D

Explanation:

"Confidential information discussed during a strategic teleconference was intercepted by the organization's top competitor." is the incident most directly addressed by encrypting data in transit over the organization's wireless network. Wireless communications propagate through radio signals and may be captured by an unauthorized party within range unless effective cryptographic protections are applied. Transport-layer encryption protects the confidentiality of communications while they traverse a network by making captured traffic unintelligible to an interceptor that lacks the required cryptographic keys. In this scenario, interception of a sensitive teleconference is a clear confidentiality breach involving data in transit, so strengthening encryption at the wireless transport level is an appropriate corrective control and helps reduce the likelihood that future communications can be read if intercepted.

NIST's guidance on wireless-network security emphasizes the need to protect wireless transmissions from eavesdropping and unauthorized disclosure through appropriate encryption and authentication controls. See NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks. NIST also describes cryptography as a means of protecting information from unauthorized disclosure in FIPS 197, Advanced Encryption Standard.

QUESTION NO: 13

A retailer uses a third-party analytics provider to measure how visitors use its mobile application. The provider receives device identifiers, event logs and approximate location data.

Which measures would best help the retailer manage privacy risk associated with this arrangement?

A. Define permitted processing and security requirements in a written agreement.

B. Evaluate whether each category of analytics data is necessary.

C. Rely on the provider's public privacy notice as the sole control.

D. Allow the provider to use the data for any future product development.

ANSWER: A B

Explanation:

A written agreement should define the analytics provider's permitted processing activities, including the specific purposes for which data may be used, security obligations, restrictions on onward disclosure, and deletion or return requirements. Contractual terms establish enforceable boundaries for the provider's handling of information rather than relying solely on the provider's public privacy notice.

The retailer should also evaluate whether each data element is necessary for the defined analytics purpose. Reducing unnecessary event fields, limiting the precision of location information, or avoiding collection of persistent identifiers where less intrusive alternatives are sufficient can materially reduce privacy risk. These practices reflect data minimization and accountable third-party governance. The NIST Privacy Framework addresses managing privacy risks arising from data processing and ecosystem relationships: NIST Privacy Framework.

QUESTION NO: 14

When analyzing user data, how is differential privacy applied?

A. By injecting noise into aggregated datasets.

B. By assessing differences between datasets.

C. By applying asymmetric encryption to datasets.

D. By removing personal identifiers from datasets.

ANSWER: A

Explanation:

Differential privacy is applied by injecting carefully calibrated random noise into aggregated datasets. More precisely, the noise is typically added to the results of statistical queries, such as counts, sums, averages, or model-training updates, rather than indiscriminately altering the underlying source records. This makes the published aggregate useful for identifying population-level patterns while limiting what an observer can infer about whether any particular person's data was included in the analysis.

The privacy guarantee is defined by the idea that the output of an analysis should be nearly the same whether an individual's record is present or absent. The amount and distribution of noise are selected according to the sensitivity of the query and a privacy parameter, commonly called epsilon. A smaller epsilon provides a stronger privacy guarantee but can reduce analytical accuracy. This approach enables organizations to derive value from user data while reducing the risk that aggregate results reveal information about a specific individual. The U.S. Census Bureau describes differential privacy as injecting noise into statistical outputs to protect respondent confidentiality, and NIST explains its role in privacy-preserving data analysis. See the U.S. Census Bureau's differential privacy overview and NIST's differential privacy primer.

QUESTION NO: 15

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: D

Explanation:

Reviewing the code against Open Web Application Security Project (OWASP) Top 10 Security Risks is the least effective privacy-preserving practice because it is principally an application-security activity rather than a privacy-engineering activity.

The OWASP Top 10 helps development teams identify common web-application security weaknesses, such as broken access control, injection, and security misconfiguration. Addressing those weaknesses is valuable and can indirectly support privacy by reducing the likelihood of unauthorized disclosure or compromise.

However, a privacy-preserving SDLC requires practices specifically aimed at understanding and governing personal-data processing: identifying what personal data is collected, where it moves, why it is used, how long it is retained, and which privacy risks arise from the intended use case. A review limited to the OWASP Top 10 does not, by itself, assess such issues as data minimization, purpose limitation, excessive collection, inappropriate sharing, or retention. It therefore provides a narrower and more indirect privacy benefit than privacy-focused design and analysis practices. OWASP describes the Top 10 as an awareness document for web-application security risks: OWASP Top 10. Privacy engineering guidance likewise emphasizes embedding privacy requirements and controls throughout the system life cycle: NIST Privacy Engineering.

QUESTION NO: 16

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: C

Explanation:

Identity theft and embarrassment. correctly illustrates Ryan Calo's two broad dimensions of privacy harm: objective harm and subjective harm. Objective harms are concrete, externally observable adverse consequences that can result from misuse of personal information. Following an email-account takeover, an attacker may obtain enough identifying data, account-recovery details, financial communications, or contacts to impersonate the person and commit identity theft. That is a tangible consequence with real-world effects on the affected individual.

Embarrassment illustrates subjective harm. Calo uses this category for the mental, emotional, and dignitary impact created by an individual's perception that personal information has been exposed, observed, or used in an unwanted way. A compromised email account can reveal private messages, attachments, and sensitive exchanges, leaving the account holder distressed or embarrassed even where the harm is not readily measurable in financial terms. Together, identity theft supplies the concrete, objective dimension and embarrassment supplies the subjective, experiential dimension. This distinction helps privacy technologists assess both measurable downstream misuse and the personal impact of unwanted exposure when designing incident response and safeguards.

See Ryan Calo, The Boundaries of Privacy Harm, and the published article at the Indiana Law Journal.

QUESTION NO: 17

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.

ANSWER: B C

Explanation:

Machine-learning systems can create privacy and data-protection risks when **"The solution may contain inherent bias from the developers."** Design decisions made by development teams—including the selection of features, labels, objectives, and thresholds—can embed assumptions that produce unfair or discriminatory outcomes for individuals or groups. Bias can also arise through the data and processes chosen by those teams, making governance, testing, and impact assessment important throughout the system lifecycle.

"The decision-making process used by the solution is not documented." is also a privacy risk because documentation supports transparency, accountability, auditability, and meaningful explanations of automated processing. Without records of how the model was designed, trained, evaluated, deployed, and monitored, an organization may be unable to demonstrate responsible processing, investigate harmful outcomes, or provide appropriate information to affected individuals. Privacy-enhancing AI governance therefore includes documented decision processes, clear accountability, and ongoing evaluation for bias and other impacts. The IAPP's AI Governance Center emphasizes responsible AI governance, while the NIST AI Risk Management Framework identifies documentation and transparency as key practices for managing AI risks. See the IAPP AI Governance Center and NIST AI Risk Management Framework.

QUESTION NO: 18

A company is designing a customer portal that will allow users to download account statements containing personal and financial information.

Which controls would best support the principle of least privilege for employee access to those statements?

A. Assign permissions based on defined job roles.

B. Review employee access when job responsibilities change.

C. Provide all portal administrators with statement-viewing access.

D. Use a shared support account for all customer-service employees.

ANSWER: A B

Explanation:

Role-based access control supports least privilege by assigning permissions according to defined job responsibilities. For example, a customer-service representative may need to view a statement to resolve an inquiry, while a system administrator may need to maintain the portal without having routine access to statement content. Separating these permissions reduces unnecessary access to personal information.

Periodic access reviews are also important because access that was initially appropriate can become excessive when an employee changes jobs, assumes new responsibilities, or leaves the organization. Reviewing assigned roles and removing unneeded privileges helps ensure that access remains limited to current business needs. NIST describes least privilege as restricting access to the minimum necessary to accomplish assigned tasks in its glossary definition.

QUESTION NO: 19

When should code audits be concluded?

A. At code check-in time.

B. At engineering design time.

C. While code is being sent to production.

D. Before launch after all code for a feature is complete.

ANSWER: D

Explanation:

Code audits should be concluded before launch, after all code for the feature is complete. At that point, reviewers can assess the complete implementation rather than an incomplete snapshot: application logic, data flows, integrations, configuration, error handling, and privacy-relevant processing behavior can be evaluated together. This provides a meaningful basis for determining whether the feature implements the intended security and privacy requirements and whether any findings have been remediated or formally accepted before the feature affects production users or personal data.

This timing does not imply that secure coding review begins only at the end of development. Effective software-development practices incorporate review activities throughout implementation, while a final audit conclusion occurs when the full feature is available and before release. NIST's Secure Software Development Framework calls for verification of software security requirements and remediation of identified vulnerabilities before release. OWASP similarly describes code review as a means of identifying security issues in the implemented application. Completing the audit before launch preserves time to correct issues and document release readiness without exposing production environments to unreviewed feature code. See NIST SP 800-218, Secure Software Development Framework and the OWASP Code Review Guide.

QUESTION NO: 20

To comply with the Sarbanes-Oxley Act (SOX), public companies in the United States are required to annually report on the effectiveness of the auditing controls of their financial reporting systems. These controls must be implemented to prevent unauthorized use, disclosure, modification, and damage or loss of financial data.

Why do these controls ensure both the privacy and security of data?

A. Modification of data is an aspect of privacy; unauthorized use, disclosure, and damage or loss of data are aspects of security.

B. Unauthorized use of data is an aspect of privacy; disclosure, modification, and damage or loss of data are aspects of security.

C. Disclosure of data is an aspect of privacy; unauthorized use, modification, and damage or loss of data are aspects of security.

D. Damage or loss of data are aspects of privacy; disclosure, unauthorized use, and modification of data are aspects of privacy.

ANSWER: C

Explanation:

"Disclosure of data is an aspect of privacy; unauthorized use, modification, and damage or loss of data are aspects of security" is correct because privacy and security address related but distinct risks. Privacy is concerned with the appropriate handling of information and, particularly, whether information is revealed or shared in a way that is authorized and consistent with applicable obligations. Preventing improper disclosure therefore protects the privacy interests associated with financial data, including information that may identify individuals or reveal sensitive business details.

Security provides the safeguards that preserve information and systems against threats. Controls that prevent unauthorized use protect against improper access or operation of financial-reporting systems. Controls that prevent modification support data integrity, ensuring records remain accurate and reliable for reporting and audit purposes. Controls preventing damage or loss support availability and resilience, ensuring that financial information remains accessible and recoverable when needed. Together, these safeguards help a public company maintain trustworthy financial reporting while limiting inappropriate exposure of information. The IAPP describes privacy as involving the responsible handling of personal information, while NIST's information-security concepts address protection from unauthorized use, modification, destruction, and disclosure. See the IAPP overview of privacy and the NIST definition of information security.

QUESTION NO: 21

A privacy engineer is reviewing a proposed data-sharing interface between a company and a business partner.

Which interface controls would best help prevent unauthorized disclosure of personal information?

A. Authenticate the partner system before permitting interface access.

B. Restrict the partner to approved data fields and functions.

C. Provide the partner with a shared administrative credential.

D. Allow the partner to query all customer records for future use.

ANSWER: A B

Explanation:

Strong authentication of the partner system helps ensure that only an approved entity can initiate requests to the interface. Authentication should be paired with credentials that are securely managed, limited in scope, and rotated or revoked when the relationship changes.

Authorization controls that restrict the partner to approved data fields and functions are equally important. An authenticated partner should not automatically receive every category of information available through an interface. Limiting the fields, records, and operations available to the partner enforces purpose limitation and reduces the impact of a compromised credential or application error. OWASP recommends applying both authentication and authorization controls to APIs in its API Security Project.

QUESTION NO: 22

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:

• "I consent to receive notifications and infection alerts";

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

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

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

• "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:

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

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

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

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

• 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 ON default setting for consent to receive potential marketing information.

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

ANSWER: A C

Explanation:

The ON or OFF default setting for each item is a major privacy-by-design concern because every sharing purpose begins enabled, including purposes involving highly sensitive health, location, and risk-status information. A meaningful consent choice requires an affirmative, informed user action; an interface that presumes agreement and requires users to locate and turn off each separate purpose is an opt-out design rather than privacy-protective default behavior. Privacy by default calls for the least privacy-invasive settings until a person actively chooses otherwise.

The ON default setting for consent to receive information on additional features or services, and new products is particularly concerning because it makes marketing-related communications dependent on presumed consent. Marketing is separate from the core screening and exposure-notification service, so a user should be able to make a distinct, voluntary opt-in decision without losing access to essential health functionality. This separation supports purpose limitation and avoids conditioning service use on unnecessary promotional processing.

The FTC has emphasized that businesses handling sensitive data, including health and precise location information, should obtain affirmative express consent before using or disclosing it beyond necessary purposes. Its privacy guidance also supports building privacy protections into product design and default settings. See the FTC Policy Statement on Location and Health Information and the NIST Privacy Framework.

QUESTION NO: 23

Which of the following is the primary privacy benefit of separating production and test environments?

A. It limits access to production personal data by development and testing personnel.

B. It eliminates the need to authenticate users in the production environment.

C. It permits developers to retain production data indefinitely for troubleshooting.

D. It ensures that all test data is anonymous.

ANSWER: A

Explanation:

It limits access to production personal data by development and testing personnel. Separating environments enables an organization to restrict production information to systems and personnel that require it for live business operations. Developers and testers can work in a distinct environment using synthetic, masked, or appropriately de-identified data rather than obtaining broad access to live customer records.

This separation reduces the number of people, systems, and vendors exposed to production data and helps prevent test activity from changing, disclosing, or retaining live records. It also supports stronger access governance, monitoring, and change-control practices. OWASP recommends keeping development, test, and production environments separate as part of secure application design; see the OWASP Infrastructure as Code Security Cheat Sheet.

QUESTION NO: 24

A company permits employees to work remotely using managed laptops that may contain customer information.

Which controls would best reduce privacy and security risks if a laptop is lost or stolen?

A. Enable full-disk encryption.

B. Require strong authentication to unlock the device.

C. Use remote-device management and wipe capabilities.

D. Suppress the wireless network name.

ANSWER: A B C

Explanation:

Full-disk encryption helps protect data at rest by making the laptop's storage unreadable to an unauthorized person who obtains the device. Strong authentication helps protect the keys or credentials needed to access the encrypted information. Remote-device management can support timely actions such as locating a device, revoking access or remotely wiping organizational data when appropriate.

These measures should be supported by clear reporting procedures so that a lost device is promptly assessed and managed. Simply hiding the wireless network name does not protect personal information stored on an endpoint device. See NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices and NIST SP 800-46 Rev. 2.

QUESTION NO: 25

An organization is considering a new system that will combine customer purchase histories with third-party demographic data to create marketing segments.

Which factors would indicate that a privacy impact assessment should be performed before deployment?

A. The system will generate inferences by combining datasets.

B. The system will profile individuals for marketing segments.

C. The demographic data will be obtained from a third party.

D. The system will use a standard relational database.

ANSWER: A B C

Explanation:

Combining datasets to create new inferences about individuals can create privacy risks that are not apparent when each dataset is considered separately. The proposed use also involves profiling individuals for marketing decisions, which can affect expectations, transparency and the potential for inappropriate or unfair outcomes.

Sharing personal data with a third party introduces additional risks involving the source, accuracy, contractual controls, permitted uses, onward disclosures and security of the combined data. A privacy impact assessment helps the organization identify these risks and determine mitigations before processing begins.

The ICO explains that a data protection impact assessment is particularly relevant when processing is likely to result in a high risk to individuals, including profiling and matching or combining datasets. See the ICO guidance on when a DPIA is needed.

QUESTION NO: 26

Which of the following scenarios best exemplifies the concept of Privacy by Default?

A. An organization develops a website to provide customers the ability to purchase products and the choice to opt-in to personalized health marketing based off the products they purchase.

B. An internal team builds a product that will perform analysis on employee site usages by leveraging the data loss prevention tool and use that to block popular risky websites.

C. A business engages a third party vendor to install cameras in the store to identify criminal behavior and stop criminals as soon as possible to protect customers.

D. A software team realizes the product they have already built could potentially have privacy concerns and before deploying it, they request a meeting to get the privacy team ' s input.

ANSWER: A

Explanation:

“An organization develops a website to provide customers the ability to purchase products and the choice to opt-in to personalized health marketing based off the products they purchase.” best exemplifies Privacy by Default because the site can deliver its core purchasing function without automatically enabling the additional, more privacy-invasive use of purchase data for personalized marketing. Personalized health marketing is available only when the customer takes an affirmative action to opt in. This design places the more protective setting first: no marketing personalization occurs unless the individual chooses it.

Privacy by Default is a foundational Privacy by Design principle: privacy-protective settings should apply automatically, so individuals do not need to discover and change settings to avoid unnecessary collection, use, or disclosure. The principle supports data minimization and purpose limitation by restricting processing to what is needed for the default service unless the person deliberately enables an optional feature. This approach is also reflected in GDPR Article 25, which requires controllers to implement measures ensuring that, by default, only personal data necessary for each specific purpose are processed. See the Seven Foundational Principles of Privacy by Design and GDPR Article 25.

QUESTION NO: 27

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

The app is designed to collect and transmit geolocation data. How can data collection best be limited to the necessary minimum?

A. Allow user to opt-out geolocation data collection at any time.

B. Allow access and sharing of geolocation data only after an accident occurs.

C. Present a clear and explicit explanation about need for the geolocation data.

D. Obtain consent and capture geolocation data at all times after consent is received.

ANSWER: A B

Explanation:

Allowing a user to opt out of geolocation collection at any time supports data minimization by giving the individual a practical control to stop collection when location data is no longer needed. For an accident-claim app, ongoing location tracking is generally unnecessary once the relevant incident information has been captured. A privacy-protective implementation should make this control easy to find and use, and should stop associated collection and transmission promptly when the user exercises it.

Limiting access and sharing of geolocation data to the period after an accident occurs also directly aligns collection and use with the app's defined claims purpose. The app needs location information to document the crash site and support assessment of a particular claim, rather than to maintain a continuous record of a person's movements. Designing collection so that it is event-based, scoped to the accident, and limited in duration reduces the volume of personal data processed while retaining information necessary for the insurance workflow.

This approach reflects privacy-by-design data-minimization practices: collect personal data that is adequate, relevant, and limited to what is necessary for the stated purpose. The IAPP's privacy engineering resources discuss embedding such controls into product design, while the UK ICO provides practical guidance on the data-minimisation principle. See IAPP Privacy Engineering and ICO data minimisation guidance.

QUESTION NO: 28

An organization is using new technologies that will target and process personal data of EU customers. In which of the following circumstances would a privacy technologist need to support a data protection impact assessment (DPIA)?

A. If a privacy notice and opt-m consent box are not displayed to the individual

B. If security of data processing has not been evaluated

C. If a large amount of personal data will be collected.

D. If data processing is a high risk to an individual's rights and freedoms

ANSWER: D

Explanation:

If data processing is a high risk to an individual's rights and freedoms, a privacy technologist would need to support a data protection impact assessment (DPIA). Article 35 of the GDPR requires a DPIA before processing where, particularly when using new technologies and considering the nature, scope, context, and purposes of processing, it is likely to result in a high risk to natural persons' rights and freedoms. The assessment is a forward-looking accountability measure: it documents the planned processing, assesses its necessity and proportionality, identifies risks to individuals, and specifies measures to address those risks. A privacy technologist can make a key contribution by describing data flows, technical architecture, access controls, security safeguards, retention mechanisms, and privacy-enhancing measures. The use of new technology can be an important indicator, but it is the likelihood of high risk that triggers the DPIA requirement. The controller remains responsible for ensuring that the DPIA is performed, and must consult the supervisory authority before processing if residual high risk cannot be sufficiently mitigated. See GDPR Article 35 at EUR-Lex and the European Data Protection Board's DPIA guidance.

QUESTION NO: 29

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

ANSWER: D

Explanation:

Individual participation is correct. This privacy principle recognizes that people should have meaningful involvement with personal data about them that an organization holds. A central element is the ability to obtain information about one's data, challenge its accuracy or completeness, and have it corrected, completed, amended, or erased when the challenge succeeds. These rights help ensure that personal information used in decisions, services, and records remains accurate and reflects the individual's circumstances.

The principle originates in the OECD Privacy Guidelines. Under the Individual Participation Principle, an individual should be able to learn whether a controller holds data relating to them, obtain that data within a reasonable time and in an intelligible form, challenge a denial of access, and challenge data relating to them. If the challenge is successful, the data should be erased, rectified, completed, or amended. This is closely reflected in modern privacy laws' rights of access, rectification, and erasure. See the OECD Privacy Guidelines and the GDPR's rights to rectification and erasure.

QUESTION NO: 30

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: B D

Explanation:

Conducting a security and privacy review before onboarding new vendors that collect personal data from the app is an essential vendor-governance control. EnsureClaim is disclosing a substantial range of personal data, including identity information, photographs, insurance details, vehicle information, and geolocation data. Before a hosting or other service provider receives that information, EnsureClaim should assess the provider's privacy practices, security architecture, access controls, encryption, incident-response capabilities, retention and deletion practices, and ability to meet contractual and legal obligations. This due diligence helps establish that the provider can appropriately protect the data throughout the processing relationship.

Developing policies and procedures that outline how data is shared with third-party apps is also appropriate because supervision needs repeatable internal controls, not only a one-time assessment. Documented procedures can specify approved recipients, categories of data permitted for disclosure, authorization and review requirements, contractual safeguards, secure transfer methods, and periodic reassessment or monitoring. Together, pre-onboarding reviews and operational data-sharing procedures provide a defensible framework for managing third-party risk. NIST's supply-chain risk-management guidance supports integrating supplier security requirements and assessment activities into organizational processes: NIST SP 800-161 Rev. 1. Guidance on controller-processor arrangements likewise emphasizes documented instructions and sufficient guarantees from processors: ICO guidance on controller-processor contracts.