PassQueen
a.k.a dumpsqueen.com

Certified Information Privacy Professional/ Canada (CIPP/C)

IAPP CIPP-C

Version Demo

Total Demo Questions: 24

Total Premium Questions: 244

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to the Canadian Legal System	13
Topic 2, Canadian Privacy Legislation and Jurisprudence	12
Topic 3, Public Sector Privacy Laws	21
Topic 4, Private Sector Privacy Laws	96
Topic 5, Canada's Health Privacy Laws	16
Topic 6, Mix Questions	86
Total	244

QUESTION NO: 1

What is the Generally Accepted Privacy Principles (GAPP) framework?

A. An information management model that is widely recognized across many Canadian industries.

B. A comprehensive guide for industry best practices as delineated by the Canadian federal Privacy Commissioner.

C. A template for Privacy Impact Assessments (PIAs) that are conducted within private sector organizations in Canada.

D. A principles-based privacy approach advocated by Canada's leading accounting industry group and its U.S.-based counterpart.

ANSWER: D

Explanation:

The Generally Accepted Privacy Principles (GAPP) framework is correctly described as a principles-based privacy approach advocated by Canada's leading accounting industry group and its U.S.-based counterpart. GAPP was developed jointly by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants, the predecessor organization to CPA Canada. It was designed to provide organizations with a coherent, accountable approach to managing personal information throughout its life cycle.

The framework organizes privacy management around recognized principles, including management responsibility, notice, choice and consent, collection, use and retention, access, disclosure to third parties, security, quality, monitoring and enforcement. Its purpose is to help an organization establish, assess and demonstrate privacy controls and governance practices, rather than to prescribe a particular statutory compliance process or a single assessment template. This makes it useful as an accountability-oriented framework that can be adapted to an organization's operations and applicable legal obligations. The framework's accounting-profession origins and joint Canadian-U.S. development are central to its identity. See the AICPA's Generally Accepted Privacy Principles resources and the Chartered Professional Accountants of Canada.

QUESTION NO: 2

What is the main challenge financial institutions face when managing user preferences?

A. Ensuring they are in compliance with numerous complex state and federal privacy laws

B. Developing a mechanism for opting out that is easy for their consumers to navigate

C. Ensuring that preferences are applied consistently across channels and platforms

D. Determining the legal requirements for sharing preferences with their affiliates

ANSWER: C

Explanation:

Ensuring that preferences are applied consistently across channels and platforms is the central operational challenge because a financial institution may collect and use a customer's choices through many interconnected systems: online banking, mobile applications, call centres, branch interactions, marketing tools, customer-relationship platforms, and third-party service providers. A preference is meaningful only when it is accurately recorded, propagated to the appropriate systems, and honored whenever the institution communicates with or uses information about that consumer. This requires reliable identity matching, timely synchronization, clear preference taxonomy, auditability, and controls that prevent a consumer from receiving a communication or data use that conflicts with the choice they expressed elsewhere.

Canadian privacy accountability principles reinforce the need for organizations to implement practices and safeguards that give effect to consent choices throughout their operations. In the financial-services context, this must be supported by governance and technology capable of maintaining a consistent, demonstrable preference state across the full customer journey. The Office of the Privacy Commissioner of Canada explains that meaningful consent must be implemented through organizational practices, while financial institutions subject to federal regulation must also meet privacy obligations under PIPEDA. See the OPC's Guidelines for obtaining meaningful consent and the Personal Information Protection and Electronic Documents Act.

QUESTION NO: 3

Most states with data breach notification laws indicate that notice to affected individuals must be sent in the “most expeditious time possible without unreasonable delay.” By contrast, which of the following states currently imposes a definite limit for notification to affected individuals?

A. Maine

B. Florida

C. New York

D. California

ANSWER: B

Explanation:

Florida is correct because its data-breach notification statute establishes a specific outside deadline rather than relying solely on a general promptness standard. A covered entity must provide notice to affected individuals no later than 30 days after it determines, or has reason to believe, that a breach of security has occurred. This is a definite statutory time limit and therefore fits the question’s contrast with notification rules framed only as occurring without unreasonable delay. The statute permits a limited extension of up to 15 additional days for good cause, provided that the entity gives written notice to the Florida Department of Legal Affairs within the original 30-day period. The existence of a narrowly defined extension does not remove the law’s definite deadline; it confirms that Florida uses a prescribed timetable for individual notification. Florida’s statutory requirements are set out in the Florida Information Protection Act, particularly section 501.171(4), available through the Florida Legislature’s official statutory text. The IAPP also provides jurisdictional resources on U.S. state privacy and breach-notification requirements through its U.S. State Privacy Legislation Tracker.

QUESTION NO: 4

Although an employer may have a strong incentive or legal obligation to monitor employees’ conduct or behavior, some excessive monitoring may be considered an intrusion on employees’ privacy? Which of the following is the strongest example of excessive monitoring by the employer?

A. An employer who installs a video monitor in physical locations, such as a warehouse, to ensure employees are performing tasks in a safe manner and environment.

B. An employer who installs data loss prevention software on all employee computers to limit transmission of confidential company information.

C. An employer who installs video monitors in physical locations, such as a changing room, to reduce the risk of sexual harassment.

D. An employer who records all employee phone calls that involve financial transactions with customers completed over the phone.

ANSWER: C

Explanation:

“An employer who installs video monitors in physical locations, such as a changing room, to reduce the risk of sexual harassment.” is the strongest example of excessive monitoring because a changing room is a setting where employees have an exceptionally high and objectively reasonable expectation of privacy. Video surveillance there can capture employees while changing clothes or otherwise in states of undress, creating a serious intrusion into personal dignity and bodily privacy. Even where an employer has a genuine obligation to prevent harassment and maintain a safe workplace, Canadian privacy principles require collection, use, and disclosure of personal information to be limited to what is necessary and proportionate to the identified purpose. Surveillance must therefore be assessed not only by the legitimacy of its objective, but also by the sensitivity of the location, the degree of intrusion, and whether less privacy-invasive measures could reasonably achieve the objective. A camera in a changing room is highly privacy-invasive and would require an extraordinarily compelling justification; ordinarily, preventative policies, training, reporting channels, supervision, and targeted investigations are more

proportionate approaches. This conclusion is consistent with the accountability, necessity, and limiting-collection principles in PIPEDA and the Office of the Privacy Commissioner of Canada's guidance on privacy in the workplace.

QUESTION NO: 5

In which situation could a request for access to one's personal information be denied under the Privacy Act?

A. The personal information was collected by the Royal Canadian Mounted Police while performing policing services for a province or municipality.

B. The personal information was obtained in confidence from a foreign state or agency which has consented to the disclosure of the information.

C. The release of the personal information could reasonably be expected to cause injury to a protected species of wildlife.

D. The personal information is more than 20 years old and relates to the detection or suppression of money laundering.

ANSWER: A

Explanation:

The personal information was collected by the Royal Canadian Mounted Police while performing policing services for a province or municipality. This reflects the special protection in subsection 22(3) of Canada's *Privacy Act*. Subject to the statutory conditions, this provision requires the head of a federal government institution to refuse access to personal information obtained or prepared by the Royal Canadian Mounted Police while it is providing provincial or municipal policing services under an arrangement made under the *Royal Canadian Mounted Police Act*. The rule recognizes that records generated through contract policing can be governed by the relevant province's or municipality's interests and access regime, rather than being disclosed through a federal Privacy Act request. The statutory exception permits disclosure where the province or municipality concerned consents. Thus, this is a recognized circumstance in which an individual's access request may be refused under the federal Privacy Act. The governing exemption is set out in section 22(3) of the Privacy Act; the authority for provincial and municipal policing arrangements appears in section 20 of the Royal Canadian Mounted Police Act.

QUESTION NO: 6

According to the Privacy Act, which of the following disclosures of personal information by a government institution would require the data subject's consent?

A. When disclosing to a law enforcement body.

B. When disclosing to comply with a search warrant.

C. When disclosing to a registered charitable organization.

D. When disclosing to a member of parliament to assist in resolving a problem.

ANSWER: C

Explanation:

"When disclosing to a registered charitable organization" is the disclosure that would require the individual's consent, unless the institution can establish that a separate, specific statutory exception applies. The federal *Privacy Act* establishes consent as the general rule: a government institution may disclose personal information under its control only with the consent of the individual to whom it relates. Section 8(2) then sets out a defined list of circumstances in which disclosure may occur without consent. A disclosure to a charity is not, simply because the recipient is a registered charitable organization, one of those listed circumstances. Consequently, an institution cannot treat charitable status as authorization to share an individual's personal information. It would need the individual's meaningful consent or a properly applicable authority under the Act, such as a disclosure for a use consistent with the original collection purpose or an exceptional public-interest determination made by the head of the institution. The applicable baseline rule and exceptions are set out in section 8 of the *Privacy Act*: Justice

Laws—Privacy Act, section 8. The Office of the Privacy Commissioner also describes the Act as limiting federal institutions' collection, use, and disclosure of personal information: OPC—Overview of the Privacy Act.

QUESTION NO: 7

Which action is prohibited under the Electronic Communications Privacy Act of 1986?

A. Intentionally intercepting electronic communications without authorization and accessing stored communications without authorization

B. Monitoring all employee telephone calls

C. Accessing stored communications with the consent of the sender or recipient of the message

D. Monitoring employee telephone calls of a personal nature

ANSWER: A

Explanation:

Intentionally intercepting electronic communications without authorization and accessing stored communications without authorization is prohibited under the Electronic Communications Privacy Act of 1986 (ECPA). ECPA expanded federal privacy protections beyond traditional wire communications to cover electronic communications, such as email and other electronically transmitted information. Its wiretap provisions generally prohibit the intentional interception, use, or disclosure of wire, oral, or electronic communications unless a statutory exception applies, such as valid consent or appropriately authorized law-enforcement activity. The statute's Stored Communications Act component separately protects communications held in electronic storage by restricting intentional, unauthorized access to facilities through which electronic communication services are provided and to stored communications themselves. These protections distinguish the act of unlawfully obtaining communications while they are transmitted from unlawfully accessing them after they have been stored. The relevant federal provisions are codified at 18 U.S.C. §§ 2511 and 2701. See the text of the interception prohibition at Cornell Law School, 18 U.S.C. § 2511 and the Stored Communications Act access prohibition at Cornell Law School, 18 U.S.C. § 2701.

QUESTION NO: 8

SCENARIO

Please use the following to answer the next QUESTION:

Matt went into his son's bedroom one evening and found him stretched out on his bed typing on his laptop. "Doing your network?" Matt asked hopefully.

"No," the boy said. "I'm filling out a survey."

Matt looked over his son's shoulder at his computer screen. "What kind of survey?" "It's asking Questions about my opinions."

"Let me see," Matt said, and began reading the list of Questions that his son had already answered. "It's asking your opinions about the government and citizenship. That's a little odd. You're only ten."

Matt wondered how the web link to the survey had ended up in his son's email inbox. Thinking the message might have been sent to his son by mistake he opened it and read it. It had come from an entity called the Leadership Project, and the content and the graphics indicated that it was intended for children. As Matt read further he learned that kids who took the survey were automatically registered in a contest to win the first book in a series about famous leaders.

To Matt, this clearly seemed like a marketing ploy to solicit goods and services to children. He asked his son if he had been prompted to give information about himself in order to take the survey. His son told him he had been asked to give his name, address, telephone number, and date of birth, and to answer Questions about his favorite games and toys.

Matt was concerned. He doubted if it was legal for the marketer to collect information from his son in the way that it was. Then he noticed several other commercial emails from marketers advertising products for children in his son's inbox, and he decided it was time to report the incident to the proper authorities.

How does Matt come to the decision to report the marketer's activities?

A. The marketer failed to make an adequate attempt to provide Matt with information

B. The marketer did not provide evidence that the prize books were appropriate for children

C. The marketer seems to have distributed his son's information without Matt's permission

D. The marketer failed to identify himself and indicate the purpose of the messages

ANSWER: A

Explanation:

The marketer failed to make an adequate attempt to provide Matt with information. The scenario concerns the online collection of personal information from a child under 13 for a child-directed survey and marketing-related contest. Under the U.S. Children's Online Privacy Protection Act (COPPA) Rule, an operator of a child-directed website or online service must give parents direct notice of its information practices before collecting, using, or disclosing a child's personal information, and generally must obtain verifiable parental consent. The information requested here—including the child's name, home address, telephone number, and date of birth—is personal information covered by the Rule. A notice that reaches the child, rather than an adequate direct notice to the parent, does not fulfill the operator's parental-notice obligation. Matt's discovery that his son supplied this information without prior parental notification gives him a sound basis to report the matter to the appropriate regulator. The Federal Trade Commission explains that covered operators must provide direct notice to parents and obtain verifiable parental consent before collection in most circumstances: FTC COPPA FAQs. The Rule's notice and consent requirements are set out at 16 CFR Part 312.

QUESTION NO: 9

Which of the following describes a difference between the federal Privacy Commissioner and provincial commissioners?

A. Provincial commissioners can order an organization to act.

B. Provincial commissioners are limited to recommending actions.

C. The federal commissioner has the power to make an organization comply.

D. The federal commissioner must receive complaints from a legislative representative.

ANSWER: A

Explanation:

Provincial commissioners can order an organization to act. This captures an important distinction in the enforcement models applicable to private-sector privacy regulation in Canada. The privacy commissioners of Alberta and British Columbia, for example, may issue binding orders following an inquiry under their respective private-sector privacy statutes. Such orders can require an organization to provide access to personal information, correct information-handling practices, stop collecting, using, or disclosing information in a specified manner, or otherwise comply with the statute. The federal Privacy Commissioner's principal role under the federal *Personal Information Protection and Electronic Documents Act* is instead ombudsman-based: the Commissioner investigates complaints and issues findings and recommendations. Where a matter is unresolved, the complainant or the Commissioner may apply to the Federal Court for remedies; the Commissioner does not ordinarily issue a directly binding compliance order under PIPEDA. This difference matters when assessing an organization's regulatory exposure and its response to an investigation: a provincial inquiry may culminate in an enforceable commissioner order, whereas federal enforcement under PIPEDA generally requires the additional court-remedy process. See the Office of the Privacy Commissioner of Canada's PIPEDA compliance guidance and the Alberta OIPC's published orders.

QUESTION NO: 10

Work-product information is generally thought of as information about an individual that?

A. Is required by an organization to establish an employment relationship.

B. Includes internal investigation files and complaints filed about an employee.

C. Includes intellectual property developed within the scope of an employee ' s job function.

D. Is prepared or collected as part of that individual's responsibilities or activities in connection to their job.

ANSWER: D

Explanation:

"Is prepared or collected as part of that individual's responsibilities or activities in connection to their job." is correct because work-product information concerns material generated or gathered in the course of performing professional, business, or employment-related duties. The defining feature is the connection between the information and the individual's work activity: it is created, assembled, or obtained as part of carrying out responsibilities for the organization or profession. This can include records and materials reflecting the performance of assigned work, rather than information about the employee's private life or personal characteristics.

This concept is particularly important in Canadian private-sector privacy law because provincial statutes can distinguish work-product information from personal information. For example, British Columbia's Personal Information Protection Act defines work product information as information prepared or collected by an individual in the course of the individual's business, trade, or profession. Alberta's Personal Information Protection Act similarly defines the term. The phrasing in the correct response accurately captures this core legal and practical test: the information arises from, and is connected to, the person's job responsibilities or activities.

QUESTION NO: 11

An organization self-certified under Privacy Shield must, upon request by an individual, do what?

A. Suspend the use of all personal information collected by the organization to fulfill its original purpose.

B. Provide the identities of third parties with whom the organization shares personal information.

C. Provide the identities of third and fourth parties that may potentially receive personal information.

D. Identify all personal information disclosed during a criminal investigation.

ANSWER: B

Explanation:

Under the EU-U.S. Privacy Shield Framework's Notice Principle, a participating organization had to make its privacy practices transparent to individuals. This included providing notice of the types of personal information collected, the purposes for which it is used, the individual's available choices, and the types or identity of third parties to which the organization discloses that information. Accordingly, providing the identities of third parties with whom the organization shares personal information is the best answer: it reflects the framework's requirement that individuals be able to understand the onward disclosures associated with their data and make informed choices about those disclosures. The requirement supports the broader Privacy Shield accountability model, under which certified organizations remained responsible for personal information transferred to third parties in many circumstances. Although the EU-U.S. Privacy Shield Framework is no longer a valid EU transfer mechanism following the Court of Justice of the European Union's 2020 Schrems II decision, its principles remain relevant to questions addressing the historical framework and its notice obligations. See the Privacy Shield Framework principles and the FTC's Privacy Shield guidance.

QUESTION NO: 12

SCENARIO

Please use the following to answer the next QUESTION

When there was a data breach involving customer personal and financial information at a large retail store, the company's directors were shocked. However, Roberta, a privacy analyst at the company and a victim of identity theft herself, was not.

Prior to the breach, she had been working on a privacy program report for the executives. How the company shared and handled data across its organization was a major concern. There were neither adequate rules about access to customer information nor

procedures for purging and destroying outdated data. In her research, Roberta had discovered that even low- level employees had access to all of the company's customer data, including financial records, and that the company still had in its possession obsolete customer data going back to the 1980s.

Her report recommended three main reforms. First, permit access on an as-needs-to-know basis. This would mean restricting employees' access to customer information to data that was relevant to the work performed. Second, create a highly secure database for storing customers' financial information (e.g., credit card and bank account numbers) separate from less sensitive information. Third, identify outdated customer information and then develop a process for securely disposing of it.

When the breach occurred, the company's executives called Roberta to a meeting where she presented the recommendations in her report. She explained that the company having a national customer base meant it would have to ensure that it complied with all relevant state breach notification laws. Thanks to Roberta's guidance, the company was able to notify customers quickly and within the specific timeframes set by state breach notification laws.

Soon after, the executives approved the changes to the privacy program that Roberta recommended in her report. The privacy program is far more effective now because of these changes and, also, because privacy and security are now considered the responsibility of every employee.

Which principle of the Consumer Privacy Bill of Rights, if adopted, would best reform the company's privacy program?

A. Consumers have a right to exercise control over how companies use their personal data.

B. Consumers have a right to reasonable limits on the personal data that a company retains.

C. Consumers have a right to easily accessible information about privacy and security practices.

D. Consumers have a right to correct personal data in a manner that is appropriate to the sensitivity.

ANSWER: B

Explanation:

Consumers have a right to reasonable limits on the personal data that a company retains. This reflects the Consumer Privacy Bill of Rights principle of Focused Collection, under which organizations should collect only the data they need for identified purposes and retain it only for as long as necessary to fulfill those purposes. The retailer's possession of obsolete customer information dating to the 1980s illustrates the central governance failure addressed by this principle. Retaining data without a continuing business need unnecessarily expands the volume of information exposed in a breach and increases the potential harm to affected individuals, particularly where financial information is involved.

Applying reasonable retention limits requires the organization to establish and enforce a retention schedule tied to documented business, legal, and operational needs. It must identify records that have reached the end of their authorized lifecycle and securely destroy or de-identify them. This reform directly implements the recommended process for identifying outdated customer data and disposing of it securely, while reducing the organization's breach exposure over time. The White House framework describes Focused Collection as including reasonable limits on both collection and retention. The FTC likewise identifies reasonable retention and secure disposal as important elements of sound privacy practices. See the Consumer Data Privacy in a Networked World and the FTC's Protecting Personal Information: A Guide for Business.

QUESTION NO: 13

Global Manufacturing Co's Human Resources department recently purchased a new software tool. This tool helps evaluate future candidates for executive roles by scanning emails to see what those candidates say and what is said about them. This provides the HR department with an automated "360 review" that lets them know how the candidate thinks and operates, what their peers and direct reports say about them, and how well they interact with each other.

What is the most important step for the Human Resources Department to take when implementing this new software?

A. Making sure that the software does not unintentionally discriminate against protected groups.

B. Ensuring that the software contains a privacy notice explaining that employees have no right to privacy as long as they are running this software on organization systems to scan email systems.

C. Confirming that employees have read and signed the employee handbook where they have been advised that they have no right to privacy as long as they are using the organization's systems, regardless of the protected group or laws enforced by EEOC.

D. Providing notice to employees that their emails will be scanned by the software and creating automated profiles.

ANSWER: A

Explanation:

Making sure that the software does not unintentionally discriminate against protected groups is the most important implementation step because the tool is used to assess people for a high-impact employment decision: selection for executive roles. Automated analysis of email content and relationship patterns can embed or amplify historical bias, rely on proxies for protected characteristics, or produce systematically adverse results for individuals identified by prohibited grounds of discrimination. HR must therefore validate the system's inputs, scoring logic, and outcomes; test for disparate impact; establish meaningful human review; and document controls before relying on its recommendations. These safeguards support fair employment practices even where the vendor describes the product as objective or automated. Under the Canadian Human Rights Act, discriminatory employment practices based on protected grounds are prohibited in federally regulated workplaces. The Canadian Human Rights Commission also explains employers' responsibility to prevent discrimination and provide equal opportunity in employment: What is discrimination?. Privacy transparency remains important when workplace communications are monitored, but validating the system against discriminatory employment outcomes is the essential first control for an AI-supported candidate-evaluation process.

QUESTION NO: 14

Which of the following laws is NOT involved in the regulation of employee background checks?

A. The Civil Rights Act.

B. The Gramm-Leach-Bliley Act (GLBA).

C. The U.S. Fair Credit Reporting Act (FCRA).

D. The California Investigative Consumer Reporting Agencies Act (ICRAA).

ANSWER: B

Explanation:

The Gramm-Leach-Bliley Act (GLBA) is the correct answer because it is principally a U.S. financial-privacy law, rather than a law regulating the employer background-check process. The GLBA applies to financial institutions and governs how they protect and disclose consumers' nonpublic personal information. Its core requirements include providing privacy notices in applicable circumstances, limiting certain disclosures of covered financial information, and maintaining safeguards to protect that information. Although a financial institution may need to consider GLBA obligations when handling information in its own operations, the statute does not establish the notice, authorization, disclosure, or adverse-action framework used for employment background reports. Therefore, it is not ordinarily part of the legal regime specifically governing an employer's procurement and use of background checks. The Federal Trade Commission describes GLBA as requiring financial institutions to explain information-sharing practices and protect sensitive consumer data. See the FTC's Gramm-Leach-Bliley Act guidance. For comparison of the employment-screening context, the FTC identifies the Fair Credit Reporting Act as governing many employer uses of background reports in its employment background-check guidance.

QUESTION NO: 15

According to FERPA, when can a school disclose records without a student's consent?

A. If the disclosure is not to be conducted through email to the third party

B. If the disclosure would not reveal a student's student identification number

C. If the disclosure is to practitioners who are involved in a student's health care

D. If the disclosure is to provide transcripts to a school where a student intends to enroll

ANSWER: D

Explanation:

Under FERPA, an educational agency or institution may disclose personally identifiable information from education records, without prior written consent, to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure relates to the student's enrollment or transfer. Therefore, providing transcripts to a school where a student intends to enroll is a recognized FERPA exception to the general consent requirement. This exception supports practical student transfers and admissions processes by allowing the receiving institution to obtain records needed to evaluate admission, placement, and continuity of education. The disclosing school must make a reasonable attempt to notify the parent or eligible student of the disclosure unless its annual FERPA notice states that it forwards records on request to schools in which students seek or intend to enroll. FERPA's implementing regulations set out this exception at 34 C.F.R. § 99.31(a)(2), and the U.S. Department of Education summarizes it in its guidance on circumstances in which schools may disclose information without consent. See 34 C.F.R. § 99.31 and the U.S. Department of Education's FERPA disclosure guidance.

QUESTION NO: 16

A company's employee wellness portal offers an app to track exercise activity via users' mobile devices. Which of the following design techniques would most effectively inform users of their data privacy rights and privileges when using the app?

A. Offer information about data collection and uses at key data entry points.

B. Publish a privacy policy written in clear, concise, and understandable language.

C. Present a privacy policy to users during the wellness program registration process.

D. Provide a link to the wellness program privacy policy at the bottom of each screen.

ANSWER: A

Explanation:

Offer information about data collection and uses at key data entry points is the most effective technique because it delivers a just-in-time privacy notice in the context in which an individual is deciding whether to provide particular information or enable a device capability. Exercise-tracking apps can collect data repeatedly and through multiple functions, such as motion sensors, location services, account-profile fields, and integrations with other services. Contextual information at each relevant point makes the collection, intended use, available choices, and applicable privacy rights meaningful at the moment they matter, rather than requiring users to locate and interpret a general notice separately.

This approach supports meaningful consent and transparency: a person should understand the specific collection or use before submitting the data or activating the feature. The Office of the Privacy Commissioner of Canada's guidance on meaningful consent emphasizes providing key elements in a timely and prominent way, including at or before collection, and using just-in-time notices where appropriate. Its mobile-app guidance likewise recognizes the importance of clear explanations when personal information is collected through an app. See the OPC's Guidelines for obtaining meaningful consent and mobile apps privacy guidance.

QUESTION NO: 17

Felicia is also in favor of strict employee oversight. In addition to protecting the inventory, she wants to prevent mistakes during transactions, which will require video monitoring. She also wants to regularly check the company vehicle's GPS for locations visited by employees. She also believes that employees who use their own devices for work-related purposes should agree to a certain amount of supervision.

Given her high standards, Felicia is skeptical about the proposed location of the store. She has been told that many types of background checks are not allowed under California law. Her friend Celeste thinks these worries are unfounded, as long as applicants verbally agree to the checks and are offered access to the results. Nor does Celeste share Felicia's concern about state breach notification laws, which, she claims, would be costly to implement even on a minor scale. Celeste believes that

even if the business grows a customer database of a few thousand, it's unlikely that a state agency would hassle an honest business if an accidental security incident were to occur.

In any case, Celeste feels that all they need is common sense – like remembering to tear up sensitive documents before throwing them in the recycling bin. Felicia hopes that she's right, and that all of her concerns will be put to rest next month when their new business consultant (who is also a privacy professional) arrives from North Carolina.

Based on Felicia's Bring Your Own Device (BYOD) plan, the business consultant will most likely advise Felicia and Celeste to do what?

A. Reconsider the plan in favor of a policy of dedicated work devices.

B. Adopt the same kind of monitoring policies used for work-issued devices.

C. Weigh any productivity benefits of the plan against the risk of privacy issues.

D. Make employment decisions based on those willing to consent to the plan in writing.

ANSWER: C

Explanation:

"Weigh any productivity benefits of the plan against the risk of privacy issues" is the most appropriate advice because a BYOD arrangement creates a genuine business benefit while also expanding the organization's privacy and security exposure. Personally owned phones, tablets, and computers can help employees work flexibly and efficiently, but they can also contain a mixture of personal and business information. Any monitoring, mobile-device-management tool, remote-wipe capability, or access to device data therefore needs to be assessed for necessity, proportionality, and its effects on employee privacy.

Under Canadian private-sector privacy principles, an organization should identify a legitimate purpose for collecting, using, or accessing personal information, limit collection to what is necessary, and implement safeguards appropriate to the sensitivity of the information. A sound BYOD program consequently begins with a documented risk assessment and clear policies addressing permitted business use, security controls, separation of work and personal data where feasible, retention, incident response, and transparent employee notice. The consultant should help the business make an informed, proportionate decision about whether the operational gains justify the privacy risks and what controls are needed if it proceeds. See the Personal Information Protection and Electronic Documents Act and the Office of the Privacy Commissioner of Canada's mobile and online privacy guidance.

QUESTION NO: 18

Which of the following became the first state to pass a law specifically regulating the practices of data brokers?

A. Washington.

B. California.

C. New York.

D. Vermont.

ANSWER: D

Explanation:

Vermont. Vermont became the first U.S. state to enact legislation specifically regulating data brokers when it passed Act 171 in 2018, commonly called Vermont's Data Broker Regulation law. The law took effect on January 1, 2019, and established a state registration regime for covered data brokers. It requires qualifying businesses to register annually with

the Vermont Secretary of State and disclose specified information about their data-collection, sale, opt-out, and security practices. The statute also imposed minimum information-security requirements and gave the state enforcement tools intended to address risks associated with the trade in personal information.

This was a significant early development in U.S. privacy law because it addressed the data-broker business model directly rather than regulating personal-information practices only in a sector-specific context. Vermont's approach subsequently helped shape policy discussions and later data-broker laws in other jurisdictions. The Vermont Legislature's text of Act 171 identifies its purpose as regulating data brokers and sets out the registration and security obligations. See the enacted text of Vermont Act 171 and the Vermont Secretary of State's Data Broker Registry.

QUESTION NO: 19

Which of the following is an important implication of the Dodd-Frank Wall Street Reform and Consumer Protection Act?

A. Financial institutions must avoid collecting a customer's sensitive personal information

B. Financial institutions must help ensure a customer's understanding of products and services

C. Financial institutions must use a prescribed level of encryption for most types of customer records

D. Financial institutions must cease sending e-mails and other forms of advertising to customers who opt out of direct marketing

ANSWER: B

Explanation:

Financial institutions must help ensure a customer's understanding of products and services. A central consumer-protection result of the Dodd-Frank Act was the creation of the Consumer Financial Protection Bureau (CFPB), which is responsible for protecting consumers in the market for consumer financial products and services. The Act's consumer-financial-protection framework emphasizes transparent information, fair treatment, and communications that allow consumers to understand financial products, their material terms, costs, risks, and consequences. In particular, the CFPB has authority to address unfair, deceptive, or abusive acts or practices, an authority that supports the expectation that firms present product information in a manner consumers can meaningfully understand rather than obscuring important terms or misleading them about a product's operation.

This implication is especially relevant to privacy and financial-services compliance because customer-facing disclosures, product descriptions, notices, and marketing should be designed for clarity and accuracy. Firms should therefore build controls around plain-language communications and ensure that their sales and servicing practices support informed consumer decision-making. The CFPB describes its statutory role under the Consumer Financial Protection Act, enacted as part of Dodd-Frank, at CFPB: Consumer Financial Protection Act. The Act's full text is available through Congress.gov.

QUESTION NO: 20

SCENARIO

Please use the following to answer the next QUESTION:

You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.

A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals – ones that exposed the PHI of public figures including celebrities and politicians.

During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.

A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.

Which of the following would be HealthCo's best response to the attorney's discovery request?

A. Reject the request because the HIPAA privacy rule only permits disclosure for payment, treatment or healthcare operations

B. Respond with a request for satisfactory assurances such as a qualified protective order

C. Turn over all of the compromised patient records to the plaintiff's attorney

D. Respond with a redacted document only relative to the plaintiff

ANSWER: B

Explanation:

Respond with a request for satisfactory assurances such as a qualified protective order. HIPAA permits a covered entity to disclose protected health information in response to a discovery request in a judicial or administrative proceeding, but a request from opposing counsel that is not accompanied by a court order requires safeguards before disclosure. In this situation, HealthCo should obtain satisfactory assurances that the requesting party has either notified the affected individuals or sought a qualified protective order. A qualified protective order must prohibit use or disclosure of the information for purposes other than the litigation or proceeding and require the return to HealthCo or destruction of the information at the end of the proceeding. These assurances enable an appropriately limited litigation disclosure while preserving HIPAA protections for the many other patients whose information was involved in the incident. HealthCo should also disclose only the protected health information authorized and reasonably necessary for the litigation, consistent with the applicable discovery process and the terms of the protective order. The governing Privacy Rule provision is 45 C.F.R. § 164.512(e), available through the Electronic Code of Federal Regulations. HHS also summarizes these judicial-and-administrative-proceeding disclosure requirements in its HIPAA Privacy Rule guidance.

QUESTION NO: 21

Which federal law or regulation preempts state law?

A. Health Insurance Portability and Accountability Act

B. Controlling the Assault of Non-Solicited Pornography and Marketing Act

C. Telemarketing Sales Rule

D. Electronic Communications Privacy Act of 1986

ANSWER: B

Explanation:

The **Controlling the Assault of Non-Solicited Pornography and Marketing Act** (CAN-SPAM Act) is correct because it contains an express federal preemption provision for state statutes, regulations, and rules that specifically regulate commercial electronic-mail messages. Codified at 15 U.S.C. § 7707(b), this provision promotes a nationally consistent baseline for commercial-email regulation, rather than subjecting senders to a patchwork of differing state requirements. The preemption is not absolute: states retain authority to enforce laws that prohibit falsity or deception in commercial email, including traditional fraud and computer-crime laws. They may also enforce certain state laws that are not specifically directed at regulating commercial email. For privacy professionals, the practical point is that a commercial-email compliance program should be built around CAN-SPAM's federal requirements, including accurate header information, nondeceptive subject lines, identification requirements, a functioning opt-out mechanism, and prompt honoring of opt-out requests. The

statutory preemption language is available at 15 U.S.C. § 7707, and the Federal Trade Commission's compliance guidance is available at CAN-SPAM Act: A Compliance Guide for Business.

QUESTION NO: 22

Subject to limited exceptions, within what period must an organization generally respond to an individual access request under PIPEDA?

A. Ten days

B. Thirty days

C. Sixty days

D. Ninety days

ANSWER: B

Explanation:

Thirty days is correct. PIPEDA requires an organization to respond to an individual's request for access to personal information within 30 days of receiving the request. The organization may extend the time limit in specified circumstances, such as where meeting the request within 30 days would unreasonably interfere with its activities or where additional time is needed to consult with another organization. It must notify the individual of the extension within the initial 30-day period.

An access response should provide information about the individual's personal information held by the organization, its use and disclosure, and information about the source of the information where available. Access may be limited where a statutory exception applies, including where disclosure would reveal confidential commercial information or personal information about another individual. See Principle 4.9 of Schedule 1 to PIPEDA and the Office of the Privacy Commissioner of Canada's guidance on access requests.

QUESTION NO: 23

California's SB 1386 was the first law of its type in the United States to do what?

A. Require commercial entities to disclose a security data breach concerning personal information about the state's residents

B. Require notification of non-California residents of a breach that occurred in California

C. Require encryption of sensitive information stored on servers that are Internet connected

D. Require state attorney general enforcement of federal regulations against unfair and deceptive trade practices

ANSWER: A

Explanation:

California's SB 1386 is correctly identified as requiring commercial entities to disclose a security data breach concerning personal information about the state's residents. Enacted in 2002 and effective July 1, 2003, SB 1386 added California Civil Code section 1798.82, creating the first U.S. state data-breach notification requirement. The law requires any person or business that conducts business in California and owns or licenses computerized data containing a California resident's personal information to disclose a breach of the system's security to affected residents when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The statute also established key concepts that became models for later state breach-notification laws, including "personal information," "breach of the security of the system," and notice without unreasonable delay. California's Legislature describes SB 1386 as the bill that established these breach-notice obligations; the current statutory text remains available through the state's official legislative information service. See California Civil Code § 1798.82 and the California Attorney General's data breach reporting guidance.

QUESTION NO: 24

Which federal statute governs the collection, use, disclosure, retention, and disposal of personal information by most federal government institutions in Canada?

A. The Personal Information Protection and Electronic Documents Act

B. The Access to Information Act

C. The Privacy Act

D. The Canada Evidence Act

ANSWER: C

Explanation:

The Privacy Act is correct. The federal *Privacy Act* establishes rules for federal government institutions' handling of personal information. It grants individuals rights of access to personal information held by those institutions and rights to request correction of information, subject to statutory limitations.

PIPEDA generally governs personal-information handling in the course of commercial activities by private-sector organizations, while the *Access to Information Act* provides a general right of access to records held by federal institutions rather than serving as the principal statute governing federal institutions' handling of personal information. See the Privacy Act and the Treasury Board of Canada Secretariat's Privacy Act overview.