DUMPSARENA

Certified Information Privacy Professional/United States (CIPP/US)

IAPP CIPP-US

Version Demo

Total Demo Questions: 28

Total Premium Questions: 283

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to the U.S. Privacy Environment	67
Topic 2, Limits on Private-sector Collection and Use of Data	99
Topic 3, Government and Court Access to Private-sector Information	22
Topic 4, Workplace Privacy	45
Topic 5, State Privacy Laws	46
Topic 6, Mix Questions	4
Total	283

QUESTION NO: 1

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procedures for purging and destroying outdated data.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 Third, identify outdated customer information and then develop a process for securely disposing of it.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.

Based on the problems with the company's privacy security that Roberta identifies, what is the most likely cause of the breach?

A. Mishandling of information caused by lack of access controls.

B. Unintended disclosure of information shared with a third party.

C. Fraud involving credit card theft at point-of-service terminals.

D. Lost company property such as a computer or flash drive.

ANSWER: A

Explanation:

Mishandling of information caused by lack of access controls is the most likely cause because the scenario identifies unrestricted internal access as a central security deficiency. Even low-level personnel could access the complete customer-data repository, including highly sensitive financial records, without a demonstrated business need. That arrangement violates the least-privilege, or need-to-know, principle: access should be limited to the information and systems needed for an employee's assigned duties. Broad, poorly governed access substantially increases the likelihood that personal information will be improperly viewed, copied, used, or disclosed, whether through negligence or misuse by an insider. Roberta's primary recommendation to restrict access by job relevance directly addresses that identified exposure, while a separate secure database for financial information further limits the impact of inappropriate access. The company's retention of obsolete data also increases the volume of information exposed, but the facts most directly connect the breach risk to absent access rules and excessive employee permissions. The Federal Trade Commission's Safeguards Rule guidance emphasizes implementing access controls and limiting access to customer information to authorized users, and NIST describes least privilege as restricting authorized access to the minimum necessary to accomplish assigned tasks. See the FTC Safeguards Rule guidance and NIST definition of least privilege.

QUESTION NO: 2

SCENARIO Please use the following to answer the next question:

Miraculous Healthcare is a large medical practice with multiple locations in California and Nevada. Miraculous normally treats patients in person, but has recently decided to start offering telehealth appointments, where patients can have virtual appointments with on-site doctors via a phone app.

For this new initiative, Miraculous is considering a product built by MedApps, a company that makes quality telehealth apps for healthcare practices and licenses them to be used with the practices' branding. MedApps provides technical support for the app, which it hosts in the cloud. MedApps also offers an optional benchmarking service for providers who wish to compare their practice to others using the service.

Riya is the Privacy Officer at Miraculous, responsible for the practice's compliance with HIPAA and other applicable laws, and she works with the Miraculous procurement team to get vendor agreements in place. She occasionally assists procurement in vetting vendors and inquiring about their own compliance practices, as well as negotiating the terms of vendor agreements. Riya is currently reviewing the suitability of the MedApps app from a privacy perspective.

Riya has also been asked by the Miraculous Healthcare business operations team to review the MedApps' optional benchmarking service. Of particular concern is the requirement that Miraculous Healthcare upload information about the appointments to a portal hosted by MedApps.

If MedApps receives an access request under CCPA from a California-based app user, how should it handle the request?

A. MedApps should decline the request because Protected Health Information is not subject to CCPA.

B. MedApps should promptly verify the user's identity and provide the requested information.

C. MedApps should promptly forward the request to Miraculous for instructions on handling.

D. MedApps should decline the request because MedApps is not based in California.

ANSWER: C

Explanation:

MedApps should promptly forward the request to Miraculous for instructions on handling. In the described arrangement, Miraculous determines why and how the telehealth app is used in its patient relationship, while MedApps hosts, supports, and processes information in providing its contracted services. That positioning ordinarily makes Miraculous the CCPA "business" and MedApps a service provider (or, under current terminology, a service provider/contractor acting under a written agreement). The business is responsible for administering consumer privacy rights and for determining the appropriate scope of a response, including any applicable limitations, exclusions, and identity-verification process.

Forwarding the request allows Miraculous to coordinate the response through its established privacy process and give MedApps instructions consistent with their contract. CCPA regulations specifically address requests sent directly to a service provider or contractor: it may act for the business when authorized by the governing contract, or tell the consumer that the request cannot be acted on because it was sent to the service provider or contractor. Prompt escalation to Miraculous is therefore the appropriate operational step for MedApps. See California's CCPA resource page and the CCPA regulations on service providers and consumer requests.

QUESTION NO: 3

Which is an exception to the general prohibitions on telephone monitoring that exist under the U.S. Wiretap Act?

A. Call center exception

B. Inter-company communications exception

C. Ordinary course of business exception

D. Internet calls exception

ANSWER: C

Explanation:

The ordinary course of business exception is correct because the Wiretap Act's definition of an electronic, mechanical, or other device excludes certain telephone equipment supplied by a communications service provider, or furnished by a subscriber or user, when it is used in the ordinary course of that subscriber's or user's business. This statutory exclusion is commonly relevant to employers that monitor business telephone lines using ordinary telephone equipment for legitimate, routine business purposes, such as quality assurance, training, customer-service supervision, or protecting business operations.

The exception is not an unrestricted authorization to listen to or record calls. Its availability depends on the equipment involved, the nature and scope of the monitoring, and whether the practice is genuinely part of normal business operations. Organizations should define the business purpose, limit access and collection to what is appropriate for that purpose, maintain safeguards for recordings, and consider the separate requirements of applicable state wiretapping, recording-consent, employment, and privacy laws. The federal statutory language appears in the definition of "electronic, mechanical, or other device" at 18 U.S.C. § 2510. The Wiretap Act's general interception prohibition and statutory exceptions are set out at 18 U.S.C. § 2511.

QUESTION NO: 4

Which entities must comply with the Telemarketing Sales Rule?

A. For-profit organizations and for-profit telefunders regarding charitable solicitations

B. Nonprofit organizations calling on their own behalf

C. For-profit organizations calling businesses when a binding contract exists between them

D. For-profit and not-for-profit organizations when selling additional services to establish customers

ANSWER: A

Explanation:

The Telemarketing Sales Rule applies to for-profit sellers and telemarketers engaged in covered outbound telemarketing activities. This includes a for-profit organization that places charitable-solicitation calls on behalf of a nonprofit organization. The fact that the ultimate beneficiary is a charity does not exempt the paid, for-profit telefunding firm from the Rule's requirements. In this setting, the telefunding firm is acting as a telemarketer and must follow applicable TSR provisions, including required disclosures, prohibitions on deceptive or abusive practices, recordkeeping obligations, and relevant restrictions governing payment methods and calling practices.

The FTC distinguishes between the nonprofit entity making calls on its own behalf and a commercial firm hired to solicit donations. The Rule generally does not cover calls made directly by a charitable organization, but it does cover for-profit telemarketers that conduct charitable fundraising for those organizations. This distinction is important in privacy and marketing-compliance programs because vendor-led fundraising campaigns require appropriate oversight, contractual controls, and operational compliance procedures. The FTC's business guidance describes the TSR's applicability to sellers and telemarketers, including for-profit telefunders, and its dedicated charitable-solicitation guidance addresses obligations for commercial fundraisers. See the FTC's TSR compliance guidance and the FTC's charitable solicitation telemarketing guidance.

QUESTION NO: 5

Which of these organizations would be required to provide its customers with an annual privacy notice?

A. The Four Winds Tribal College.

B. The Golden Gavel Auction House.

C. The King County Savings and Loan.

D. The Breezy City Housing Commission.

ANSWER: C

Explanation:

The King County Savings and Loan would be required to provide an annual privacy notice because a savings and loan association is a financial institution subject to the Gramm-Leach-Bliley Act (GLBA) privacy requirements. A financial institution must give customers a clear and conspicuous notice describing its privacy policies and practices, including the categories of nonpublic personal information it collects, the categories of affiliates and nonaffiliated third parties with which it may disclose that information, and how customers may exercise applicable opt-out rights.

The annual-notice obligation applies to an institution's customer relationships, meaning continuing relationships involving a financial product or service. The Consumer Financial Protection Bureau's Regulation P establishes this requirement for financial institutions within its jurisdiction. In particular, 12 CFR § 1016.5 requires a financial institution to provide customers an annual privacy notice for as long as the customer relationship continues, subject to limited statutory and regulatory exceptions. Savings and loan associations are traditional depository financial institutions that maintain such ongoing customer relationships through deposit accounts, loans, and related services. The GLBA framework and Regulation P therefore make an annual privacy notice a core customer-facing privacy compliance obligation for this organization. See also the CFPB's Regulation P overview.

QUESTION NO: 6

Read this notice:

Our website uses cookies. Cookies allow us to identify the computer or device you're using to access the site, but they don't identify you personally. For instructions on setting your Web browser to refuse cookies, click here.

What type of legal choice does not notice provide?

A. Mandatory

B. Implied consent

C. Opt-in

D. Opt-out

ANSWER: D

Explanation:

The notice provides an **opt-out** choice because it directs the individual to instructions for configuring their web browser to refuse cookies. An opt-out mechanism allows processing to occur unless and until the person takes an affirmative step to decline it. Here, cookies are described as being in use by default, while the individual is given a practical method to stop or limit that use through browser controls. The choice is therefore framed as a refusal right rather than a requirement to obtain affirmative permission before placing cookies.

In the U.S. privacy context, browser-based controls have long been a recognized means by which users can exercise a choice regarding cookies and interest-based advertising technologies. The Federal Trade Commission has discussed consumer choice mechanisms for behavioral advertising, including tools that enable consumers to control tracking: FTC Self-Regulatory Principles for Online Behavioral Advertising. The Network Advertising Initiative likewise describes opt-out tools as mechanisms through which consumers can limit participating companies' interest-based advertising: NAI Consumer Opt Out. Because the notice supplies instructions to refuse cookies, it communicates an opt-out legal choice.

QUESTION NO: 7

A California resident has created an account on your company ' s online food delivery platform and placed several orders in the past month Later she submits a data subject request to access her personal information under the California Privacy Rights Act.

Based on the CPRA. which of the following data elements would your company NOT have to provide to the requestor once her identity has been verified?

A. Inferences made about the individual for the company s internal purposes

B. The loyalty account number assigned through the individuals use of the services

C. The time stamp for the creation of the individual ' s account in the platform ' s database.

D. The email address submitted by the individual as part of the account registration process.

ANSWER: A

Explanation:

Inferences made about the individual for the company s internal purposes is the correct answer. The CPRA's right-to-know provisions require a business to disclose the categories and specific pieces of personal information it has *collected* about a verified consumer. The statutory definition of "collects" covers activities such as gathering, obtaining, receiving, or accessing information about a consumer. Consequently, account-registration details, an account identifier, and records created when the account was opened are information the business collected or obtained in operating the platform and fall within the scope of a verified consumer's request.

A company-generated inference used solely internally—such as an analytical conclusion about likely food preferences, ordering habits, or predicted customer value—does not itself constitute a specific piece of information collected from or about the consumer in the same manner. Therefore, a business generally need not provide that internal inference in responding to a request for specific pieces of collected personal information. This conclusion should be applied carefully: inferences can meet the broad definition of personal information when they are used to create a consumer profile. Businesses should maintain an accurate data inventory and evaluate the purpose and use of inferred data when processing requests. See California Civil Code sections 1798.110 and 1798.140 at California Legislative Information and the California Privacy Protection Agency's CCPA regulations page.

QUESTION NO: 8

SCENARIO

Please use the following to answer the next question;

Miraculous Healthcare is a large medical practice with multiple locations in California and Nevada. Miraculous normally treats patients in person, but has recently decided to start offering tliehealth appointments, where patients can have virtual appointments with on-site doctors via a phone app

For this new initiative. Miraculous is considering a product built by MedApps, a company that makes quality teleheaith apps for healthcare practices and licenses them to be used with the practices " branding. MedApps provides technical support for the app. which it hosts in the cloud. MedApps also offers an optional benchmarking service for providers who wish to compare their practice to others using the service

Riya is the Privacy Officer at Miraculous, responsible for the practice ' s compliance with HIPAA and other applicable laws, and she works with the Miraculous procurement team to get vendor agreements in place She occasionally assists procurement in vetting vendors and inquiring about their own compliance practices. as well as negotiating the terms of vendor agreements. Riya is currently reviewing the suitability of the MedApps app from a privacy perspective.

Riya has also been asked by the Miraculous Healthcare business operations team to review the MedApps ' optional benchmarking service. Of particular concern is the requirement that Miraculous Healthcare upload information about the appointments to a portal hosted by MedAppsa

If MedApps receives an access request under CCPAfrom a California-based app user, how should It handle the request?

A. MedApps should immediately begin deleting the user ' s data.

B. MedApps should provide the privacy notice in an easily readable format

C. MedApps should decline the request because MedApps is not based In California.

D. MedApps should promptly forward the request to Miraculous for instructions on handling.

ANSWER: D

Explanation:

MedApps should promptly forward the request to Miraculous for instructions on handling. In providing the branded telehealth application, hosting, and technical support for Miraculous, MedApps processes app-user information on Miraculous's behalf. Miraculous is therefore the entity positioned to determine the purposes and means of processing and to make the substantive decision on a consumer request. A service provider or contractor must process personal information only for the limited business purposes set out in its contract and must assist the business with consumer-rights requests as required by the CCPA.

Promptly escalating the request allows Miraculous to verify the requester, identify information responsive to the request across relevant systems, assess any applicable healthcare-data limitations or exemptions, and provide the legally appropriate response. It also ensures that MedApps acts under documented instructions and within the scope of its service-provider agreement, rather than independently determining the response or disclosure. The vendor agreement should establish a practical intake and escalation process, response deadlines, secure communications, and the technical assistance MedApps must provide so Miraculous can meet its statutory obligations. California Civil Code section 1798.100 addresses contractual restrictions and assistance obligations for service providers and contractors, while the Attorney General's CCPA regulations address handling of consumer requests by service providers. See California Civil Code § 1798.100 and California Attorney General CCPA regulations.

QUESTION NO: 9

The FTC often negotiates consent decrees with companies found to be in violation of privacy principles. How does this benefit both parties involved?

A. It standardizes the amount of fines.

B. It simplifies the audit requirements.

C. It avoids potentially harmful publicity.

D. It spares the expense of going to trial.

ANSWER: D

Explanation:

"It spares the expense of going to trial." is correct because a negotiated FTC consent order resolves the agency's allegations without requiring the FTC and the company to complete a potentially lengthy administrative or judicial litigation process. The FTC benefits by conserving public enforcement resources and obtaining prompt, enforceable commitments—such as required privacy-program improvements, assessments, reporting, or prohibitions on specified practices. The company benefits from avoiding the legal fees, discovery costs, management time, uncertainty, and potential delay associated with contesting the matter through trial and appeals. A settlement does not simply end informally: after the FTC accepts a proposed consent agreement, it is placed on the public record for comment and may become a final order. A final FTC order is enforceable, and violations can expose the respondent to substantial civil penalties or other remedies. Thus, the central mutual advantage is an efficient resolution that secures compliance obligations while avoiding the costs of litigating the underlying privacy allegations. The FTC describes its nonadjudicative process for resolving matters through consent agreements in 16 C.F.R. Part 2. Its enforcement overview also explains the FTC's use of orders and enforcement mechanisms.

QUESTION NO: 10

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

E. Maine and Florida

ANSWER: E

Explanation:

Maine and Florida is the accurate answer under the states' current breach-notification statutes. Maine requires notice to affected residents as expeditiously as possible and without unreasonable delay, but expressly adds an outside deadline: notice generally must be made no later than 30 days after the breach is determined. The statute permits a delay where necessary to determine the scope of the breach and restore the integrity, security, and confidentiality of the system, or where a law-enforcement agency determines that notice would impede a criminal investigation. See Maine's statute, 10 M.R.S. § 1348.

Florida likewise establishes a defined deadline. A covered entity generally must provide notice to affected Florida residents no later than 30 days after determining that a breach occurred or is reasonably believed to have occurred. Florida allows an extension of up to 15 additional days for good cause, and it recognizes specified law-enforcement delays. The operative deadline is set out in Fla. Stat. § 501.171. Because both listed states impose an express numerical deadline, a single-state answer would not accurately reflect current law.

QUESTION NO: 11

Smith Memorial Healthcare (SMH) is a hospital network headquartered in New York and operating in 7 other states. SMH uses an electronic medical record to enter and track information about its patients.

Recently, SMH suffered a data breach where a third-party hacker was able to gain access to the SMH internal network. Because it is a HIPPA-covered entity, SMH made a notification to the Office of Civil Rights at the U.S. Department of Health and Human Services about the breach.

Which statement accurately describes SMH's notification responsibilities?

A. If SMH is compliant with HIPAA, it will not have to make a separate notification to individuals in the state of New York.

B. If SMH has more than 500 patients in the state of New York, it will need to make separate notifications to these patients.

C. If SMH must make a notification in any other state in which it operates, it must also make a notification to individuals in New York.

D. If SMH makes credit monitoring available to individuals who inquire, it will not have to make a separate notification to individuals in the state of New York.

ANSWER: A

Explanation:

If SMH is compliant with HIPAA, it will not have to make a separate notification to individuals in the state of New York. New York's breach-notification statute specifically accommodates HIPAA-regulated entities. A covered entity that provides breach notification under HIPAA is deemed to comply with New York's corresponding breach-notification requirements, rather than being required to send a duplicative, separately prescribed New York consumer notice. This treatment recognizes that HIPAA's Breach Notification Rule already establishes a detailed notification framework for protected health information, including notice to affected individuals without unreasonable delay and no later than 60 days after discovery of a breach, subject to the rule's requirements and exceptions. In practice, SMH's HIPAA compliance must include all applicable HIPAA notifications—not merely reporting to the HHS Office for Civil Rights. New York's statutory accommodation also requires the covered entity to notify the New York Attorney General within 10 days after determining that the breach occurred. The state-law provision is available at New York General Business Law § 899-aa. HIPAA's federal breach-notification obligations are summarized by HHS.

QUESTION NO: 12

Which of the following is commonly required for an entity to be subject to breach notification requirements under most state laws?

A. The entity must conduct business in the state

B. The entity must have employees in the state

C. The entity must be registered in the state

D. The entity must be an information broker

ANSWER: A

Explanation:

The entity must conduct business in the state is correct because state breach-notification statutes commonly apply to businesses or other covered entities that have a sufficient business connection to the state and that own, license, maintain, or otherwise hold covered personal information. The precise statutory language differs by jurisdiction, and the affected individuals' residency, the type of personal information involved, and the entity's role in handling that information are also important elements. Nevertheless, conducting business in the state is a common jurisdictional connection used in state privacy and breach-notification frameworks.

For example, California's breach-notification provision expressly addresses a person or business that "conducts business in California" and owns or licenses computerized data containing personal information. This illustrates why an organization does not need to be locally incorporated, registered, or employ personnel in a state before its relevant data practices can trigger notification duties. The practical compliance lesson is that organizations operating across state lines should assess breach obligations based on each state in which they conduct business and whose residents' covered data may be affected, rather than relying only on their physical offices or corporate-registration footprint. See California Civil Code § 1798.82 and the National Conference of State Legislatures' state breach-notification-law resource.

QUESTION NO: 13

Why was the Privacy Protection Act of 1980 drafted?

A. To respond to police searches of newspaper facilities

B. To assist prosecutors in civil litigation against newspaper companies

C. To assist in the prosecution of white-collar crimes

D. To protect individuals from personal privacy invasion by the police

ANSWER: A

Explanation:

The Privacy Protection Act of 1980 was drafted to respond to law-enforcement searches of news media facilities and the resulting risk that police could obtain journalists' unpublished reporting materials through ordinary search warrants. Its immediate impetus was *Zurcher v. Stanford Daily*, in which the U.S. Supreme Court held that the Fourth Amendment did not prohibit a warrant-based search of a student newspaper's newsroom merely because the newspaper itself was not suspected of committing the crime under investigation. Congress concluded that such searches could disrupt publication, expose confidential sources, and chill newsgathering. The Act therefore generally prohibits government officers and employees from searching for or seizing "work product materials" and "documentary materials" held by persons reasonably believed to have a purpose to disseminate information to the public. Rather than relying on a physical newsroom search, investigators ordinarily must use a subpoena or other process that provides notice and an opportunity for judicial review, subject to specified statutory exceptions. This press-focused legislative purpose is reflected in the statute's protections for materials possessed for public dissemination. See the Department of Justice's Privacy Protection Act guidance and the statutory text at 42 U.S.C. § 2000aa.

QUESTION NO: 14

In a case of civil litigation, what might a defendant who is being sued for distributing an employee's private information face?

A. Probation.

B. Criminal fines.

C. An injunction.

D. A jail sentence.

ANSWER: C

Explanation:

An injunction is a potential civil remedy when a defendant has distributed an employee's private information. An injunction is a court order directing a party to do something or, commonly in privacy-related disputes, to stop doing something—such as further disclosing, publishing, using, or disseminating the information at issue. Its purpose is preventive: it can limit ongoing or imminent harm where monetary relief alone may not adequately protect the employee's privacy once sensitive information is further circulated. Depending on the claim, the court may issue temporary relief while the lawsuit is pending and may later enter a permanent injunction as part of its final judgment. In U.S. civil litigation, injunctive relief is an equitable remedy distinct from criminal punishment, and it may be sought alongside damages when the legal requirements are satisfied. The Legal Information Institute describes an injunction as a court order requiring a person to do or cease doing a specified action. See Cornell Law School's Legal Information Institute: Injunction. Federal Rule of Civil Procedure 65 governs injunctions and restraining orders in federal civil cases: Federal Rule of Civil Procedure 65.

QUESTION NO: 15

SCENARIO

Please use the following to answer the next QUESTION

Otto is preparing a report to his Board of Directors at Filtration Station, where he is responsible for the privacy program. Filtration Station is a U.S. company that sells filters and tubing products to pharmaceutical companies for research use. The company is based in Seattle, Washington, with offices throughout the U.S. and Asia. It sells to business customers across both the U.S. and the Asia-Pacific region. Filtration Station participates in the Cross-Border Privacy Rules system of the APEC Privacy Framework.

Unfortunately, Filtration Station suffered a data breach in the previous quarter. An unknown third party was able to gain access to Filtration Stationâ€™s network and was able to steal data relating to employees in the companyâ€™s Human Resources database, which is hosted by a third-party cloud provider based in the U.S. The HR data is encrypted. Filtration Station also uses the third-party cloud provider to host its business marketing contact database. The marketing database was not affected by the data breach. It appears that the data breach was caused when a system administrator at the cloud provider stored the encryption keys with the data itself.

The Board has asked Otto to provide information about the data breach and how updates on new developments in privacy laws and regulations apply to Filtration Station. They are particularly concerned about staying up to date on the various U.S. state laws and regulations that have been in the news, especially the California Consumer Privacy Act (CCPA) and breach notification requirements.

What can Otto do to most effectively minimize the privacy risks involved in using a cloud provider for the HR data?

A. Request that the Board sign off in a written document on the choice of cloud provider.

B. Ensure that the cloud provider abides by the contractual requirements by conducting an on-site audit.

C. Obtain express consent from employees for storing the HR data in the cloud and keep a record of the employee consents.

D. Negotiate a Business Associate Agreement with the cloud provider to protect any health-related data employees might share with Filtration Station.

ANSWER: B

Explanation:

Ensure that the cloud provider abides by the contractual requirements by conducting an on-site audit. is the most effective measure because accountability for employee data remains with Filtration Station even when processing and storage are delegated to a cloud provider. A written agreement should impose specific privacy and security obligations, but vendor oversight is needed to validate that those requirements are actually being implemented in practice. An audit enables Filtration Station to assess the provider's key-management controls, including whether encryption keys are properly segregated from encrypted HR data, as well as privileged-access controls, logging, incident-response procedures, personnel safeguards, and remediation processes. In this scenario, the identified cause directly demonstrates why verification of operational controls is important: encryption does not provide meaningful protection if a provider administrator stores keys with the encrypted information. Audit findings also give Otto a documented basis to require corrective action, monitor completion, and report governance evidence to the Board. This is consistent with the FTC Safeguards Rule's expectation that covered organizations oversee service providers by selecting capable providers and requiring them by contract to maintain appropriate safeguards. The FTC's Safeguards Rule guidance and the NIST Cybersecurity Supply Chain Risk Management guidance both support ongoing, risk-based third-party oversight rather than reliance on contract language alone.

QUESTION NO: 16

SCENARIO

Please use the following to answer the next question;

Jane is a U.S. citizen and a senior software engineer at California-based Jones Labs, a major software supplier to the U.S. Department of Defense and other U.S. federal agencies Jane's manager, Patrick, is a French citizen who has been living in California for over a decade. Patrick has recently begun to suspect that Jane is an insider secretly transmitting trade secrets to foreign intelligence. Unbeknownst to Patrick, the FBI has already received a hint from anonymous whistleblower, and jointly with the National Secunty Agency is investigating Jane's possible implication in a sophisticated foreign espionage campaign

Ever since the pandemic. Jane has been working from home. To complete her daily tasks she uses her corporate laptop, which after each togin conspicuously provides notice that the equipment belongs to Jones Labs and may be monitored according to the enacted privacy policy and employment handbook Jane also has a corporate mobile phone that she uses strictly for business, the terms of which are defined in her employment contract and elaborated upon in her employee handbook. Both the privacy policy and the employee handbook are revised annually by a reputable California law firm specializing in privacy law. Jane also has a personal iPhone that she uses for private purposes only.

Jones Labs has its primary data center in San Francisco, which is managed internally by Jones Labs engineers The secondary data center, managed by Amazon AWS. is physically located in the UK for disaster recovery purposes. Jones Labs' mobile devices backup is managed by a mid-sized mobile delense company located in Denver, which physically stores the data in Canada to reduce costs. Jones Labs MS Office documents are securely stored in a Microsoft Office 365 data

When storing Jane's fingerprint for remote authentication. Jones Labs should consider legality issues under which of the following9

A. The Privacy Rule of the HITECH Act.

B. The California IoT Security Law (SB 327).

C. The applicable state law such as Illinois BIPA

D. The federal Genetic Information Nondiscrimination Act (GINA).

ANSWER: C

Explanation:

The applicable state law such as Illinois BIPA is correct because a fingerprint used to authenticate an employee is biometric information, and U.S. biometric-privacy obligations are principally governed by state law. Organizations must evaluate the law of every state with a relevant connection to the collection, use, storage, or employee—not merely the state of the employer's headquarters or its data centers. Illinois's Biometric Information Privacy Act is a central example. It regulates a private entity's collection, capture, purchase, receipt, or other acquisition of an individual's biometric identifier, including a fingerprint. Before collecting or obtaining that identifier, the entity generally must provide specified written disclosures, obtain a written release, maintain a publicly available retention schedule and destruction policy, and protect the data using the required reasonable standard of care. The statutory requirements appear in 740 ILCS 14, the Illinois Biometric Information

Privacy Act. Jones Labs should therefore identify the employee's relevant state residence and work location, determine whether a state biometric statute applies, document the required notices and consent where required, set a compliant retention and deletion schedule, and apply safeguards appropriate to the sensitivity of a biometric template. California also treats biometric information as personal information under its privacy framework, reinforcing the need to assess biometric-specific obligations and the broader privacy requirements applicable to workforce data; see the California Consumer Privacy Act statutory text.

QUESTION NO: 17

In which situation is a company operating under the assumption of implied consent?

A. An employer contacts the professional references provided on an applicant's resume

B. An online retailer subscribes new customers to an e-mail list by default

C. A landlord uses the information on a completed rental application to run a credit report

D. A retail clerk asks a customer to provide a zip code at the check-out counter

ANSWER: A

Explanation:

"An employer contacts the professional references provided on an applicant's resume" is the situation that reflects implied consent. Implied consent arises from a person's conduct and the reasonable expectations created by that conduct, rather than from a separate affirmative statement such as a signed authorization or checked consent box. By voluntarily identifying individuals as professional references and supplying their contact details in connection with a job application, the applicant communicates that those people may reasonably be contacted to discuss the applicant's work history, qualifications, and suitability for the role. The employer is therefore relying on consent inferred from the context and from the applicant's affirmative act of providing the references. The scope matters: the inference is limited to contacting the named references for the ordinary employment-reference purpose; it should not be stretched to unrelated collection, use, or disclosure of personal information. If an employer obtains a third-party consumer report for employment purposes, the Fair Credit Reporting Act imposes additional disclosure and written-permission requirements. That separate statutory process does not change the ordinary implication created when an applicant supplies professional references. See the FTC's employment-background-check guidance at https://consumer.ftc.gov/articles/employer-background-checks-your-rights and the U.S. Department of Justice's Privacy Act overview at https://www.justice.gov/opcl/privacy-act-1974.

QUESTION NO: 18

The â€œConsumer Privacy Bill of Rightsâ€ presented in a 2012 Obama administration report is generally based on?

A. The 1974 Privacy Act

B. Common law principles

C. European Union Directive

D. Traditional fair information practices

ANSWER: D

Explanation:

The correct answer is **Traditional fair information practices**. The Obama administration's 2012 report, *Consumer Data Privacy in a Networked World*, expressly states that the Consumer Privacy Bill of Rights is "generally based on widely accepted Fair Information Practice Principles" (FIPPs). These principles developed from foundational privacy practices and have influenced privacy frameworks in the United States and internationally. The report tailored those established practices to the networked economy by framing them as consumer-facing rights and organizational responsibilities.

The resulting framework identifies rights involving individual control over personal data, transparency regarding data practices, respect for the context in which data is provided, reasonable security, access and accuracy, focused collection, and accountability. These concepts reflect the core purpose of traditional fair information practices: ensuring that entities collecting and using personal information do so openly, responsibly, and with meaningful protections for individuals. Thus, the Consumer Privacy Bill of Rights was not presented as a restatement of one specific statute or foreign legal instrument; it was a policy framework grounded in the longstanding FIPPs tradition. The original report is available through the archived White House report. Additional historical context on FIPPs is provided by the Federal Trade Commission's privacy report.

QUESTION NO: 19

Which of the following federal agencies does NOT have regulatory authority related to privacy?

A. Consumer Financial Protection Bureau.

B. U.S. Department of Transportation.

C. U.S. Department of Commerce.

D. Federal Reserve

ANSWER: C

Explanation:

U.S. Department of Commerce. is the correct answer because it generally does not serve as a federal privacy regulator with authority to issue and enforce comprehensive consumer-privacy rules. Commerce's privacy role is principally administrative, technical, and policy-oriented. For example, its International Trade Administration administers the certification process for the EU-U.S. Data Privacy Framework, under which participating organizations self-certify their commitments. However, Commerce does not itself enforce participating organizations' privacy promises; enforcement may be undertaken by agencies with relevant statutory authority, particularly the Federal Trade Commission or, for certain air carriers, the Department of Transportation. Commerce also houses the National Institute of Standards and Technology, which develops influential voluntary resources such as the NIST Privacy Framework. These tools help organizations identify and manage privacy risks, but they are guidance rather than Commerce-issued, generally applicable privacy regulations. Thus, Commerce has an important role in facilitating international data-transfer arrangements, developing privacy standards, and advancing policy, but not the type of direct privacy-rulemaking and enforcement authority contemplated by the question. See the Department of Commerce's Data Privacy Framework Program and NIST's Privacy Framework.

QUESTION NO: 20

A student has left high school and is attending a public postsecondary institution. Under what condition may a school legally disclose educational records to the parents of the student without consent?

A. If the student has not yet turned 18 years of age

B. If the student is in danger of academic suspension

C. If the student is still a dependent for tax purposes

D. If the student has applied to transfer to another institution

ANSWER: C

Explanation:

"If the student is still a dependent for tax purposes" is correct because FERPA permits, but does not require, an educational institution to disclose education records to a parent without the eligible student's consent when the parent claims the student as a dependent for federal income-tax purposes. The applicable FERPA exception is tied to dependency as defined in section 152 of the Internal Revenue Code. Once a student attends a postsecondary institution, FERPA rights generally transfer from the parent to the student, regardless of whether the student is under age 18. Accordingly, the institution must have a reasonable basis for determining that the parent meets the federal tax-dependency condition before relying on this

exception. In practice, schools commonly establish procedures for requesting appropriate documentation or an attestation of dependency, and they should disclose only information permitted by FERPA and consistent with their policies. This exception authorizes disclosure to the qualifying parent; it does not eliminate the institution's ongoing responsibility to safeguard education records or require routine parental access. The Department of Education identifies disclosure to parents of a tax-dependent student as a permitted disclosure without consent in its FERPA guidance. See 34 C.F.R. § 99.31(a)(8) and the Department of Education's FERPA postsecondary disclosure guidance.

QUESTION NO: 21

What is the primary purpose of the Electronic Communications Privacy Act?

A. To protect the privacy of electronic communications in transit and in storage

B. To require encryption of all consumer communications

C. To establish a national data-breach notification requirement

D. To regulate unsolicited commercial email advertisements

ANSWER: A

Explanation:

The correct answer is **To protect the privacy of electronic communications in transit and in storage**. The Electronic Communications Privacy Act (ECPA) expanded federal protections for wire, oral, and electronic communications. Its Wiretap Act provisions generally restrict the intentional interception of communications, while the Stored Communications Act addresses unauthorized access to certain stored electronic communications and records held by service providers.

ECPA is important in privacy practice because emails, text messages, and other electronic communications may receive different protections depending on whether they are being transmitted or are stored with a service provider. The statute includes exceptions, including specified provider and consent exceptions, but its overall purpose is to establish privacy protections for electronic communications. See the statutory text at 18 U.S.C. Chapter 119 and 18 U.S.C. Chapter 121.

QUESTION NO: 22

Federal laws establish which of the following requirements for collecting personal information of minors under the age of 13?

A. Implied consent from a minorâ€™s parent or guardian, or affirmative consent from the minor.

B. Verifiable affirmative consent from a minor's parent or guardian before collecting the minor's personal information online.

C. Implied consent from a minorâ€™s parent or guardian before collecting a minorâ€™s personal information online, such as when they permit the minor to use the internet.

D. Affirmative consent of a parent or guardian before collecting personal information of a minor offline (e.g., in person), which also satisfies any requirements for online consent.

ANSWER: B

Explanation:

"Verifiable affirmative consent from a minor's parent or guardian before collecting the minor's personal information online" is correct because the Children's Online Privacy Protection Act (COPPA) regulates online operators' collection, use, and disclosure of personal information from children under 13. COPPA applies to operators of websites and online services directed to children, as well as operators with actual knowledge that they collect personal information online from children under 13. Before collecting such information, the operator generally must provide direct notice to the parent and obtain verifiable parental consent. The consent standard is intended to provide reasonable assurance, in light of available technology, that the person granting permission is in fact the child's parent or legal guardian. The Federal Trade Commission's COPPA Rule describes acceptable methods that may be used to obtain verifiable parental consent, subject to the nature of the information practices and associated risks. COPPA therefore establishes a meaningful prior parental-

permission requirement for covered online data collection; a child's own agreement does not substitute for that parental authorization. The FTC's Children's Privacy guidance and the text of the COPPA Rule, 16 C.F.R. Part 312 provide the governing framework.

QUESTION NO: 23

What information did the Red Flag Program Clarification Act of 2010 add to the original Red Flags rule?

A. The most common methods of identity theft.

B. The definition of what constitutes a creditor.

C. The process for proper disposal of sensitive data.

D. The components of an identity theft detection program.

ANSWER: B

Explanation:

The definition of what constitutes a creditor is correct. The Red Flag Program Clarification Act of 2010 amended the Fair Credit Reporting Act provisions underlying the Red Flags Rule by supplying a more specific statutory definition of "creditor." This clarification was important because it narrowed and clarified which entities must establish identity-theft prevention programs. Under the amendment, an entity is generally a creditor when it regularly and in the ordinary course of business obtains or uses consumer reports in connection with a credit transaction; furnishes information to consumer reporting agencies in connection with a credit transaction; advances funds to or on behalf of a person, other than for expenses incidental to a service provided by the creditor; or is a person that regularly and in the ordinary course of business advances funds. The Act also provided exclusions intended to ensure that professionals and similar service providers are not treated as creditors merely because they bill after services are performed, unless they meet the relevant statutory criteria. Thus, the Act's central addition was a definition that addresses the scope of covered creditors, rather than adding operational requirements for identifying red flags. The statute is available at Congress.gov, and the FTC's implementation guidance appears at FTC Red Flags Rule guidance.

QUESTION NO: 24

What is the main purpose of the Global Privacy Enforcement Network?

A. To promote cooperation among privacy authorities globally

B. To investigate allegations of privacy violations internationally

C. To protect the interests of privacy consumer groups worldwide

D. To arbitrate disputes between countries over jurisdiction for privacy laws

ANSWER: A

Explanation:

The Global Privacy Enforcement Network's central purpose is to promote practical cooperation among privacy enforcement authorities around the world. GPEN is a network of national and subnational data-protection and privacy regulators that supports members in addressing privacy issues that increasingly cross national borders. Its work includes sharing information and enforcement experience, developing contacts among authorities, and facilitating coordinated action where appropriate. This cooperation helps regulators handle matters involving multinational organizations and online services more effectively, since relevant evidence, affected individuals, and organizational operations may be located in several jurisdictions.

Accordingly, "To promote cooperation among privacy authorities globally" most accurately reflects GPEN's purpose. The network is designed to improve the effectiveness of privacy-law enforcement through regulator-to-regulator collaboration, rather than serving as a separate international court or advocacy organization. GPEN also conducts initiatives such as

privacy sweeps, which allow participating authorities to examine common privacy practices and exchange findings. The official GPEN website describes the network as a forum for privacy enforcement authorities to cooperate and share expertise. See the Global Privacy Enforcement Network and the OECD's Privacy Guidelines, which support international cooperation in privacy enforcement.

QUESTION NO: 25

Which of the following does Title VII of the Civil Rights Act prohibit an employer from asking a job applicant?

A. Questions about age

B. Questions about a disability

C. Questions about national origin

D. Questions about intended pregnancy

ANSWER: C

Explanation:

Questions about national origin are the best answer because Title VII prohibits employment discrimination based on national origin, as well as race, color, religion, and sex. In the hiring context, employers should not solicit an applicant's national-origin information unless a narrow, lawful, and genuinely job-related reason applies. Such questions can reveal protected characteristics, deter qualified people from applying, or provide evidence that national origin was considered in a selection decision. For example, an employer generally should focus on whether an applicant is authorized to work in the United States, rather than asking where the applicant or the applicant's family was born. The Equal Employment Opportunity Commission explains that national-origin discrimination includes unfavorable treatment because of a person's birthplace, ancestry, culture, linguistic characteristics, or association with an ethnic group. This Title VII protection applies throughout the employment relationship, including recruitment, applications, interviews, hiring, assignments, compensation, and termination. Privacy professionals and HR teams should therefore design application forms and interview guidance to collect only information necessary for a legitimate hiring purpose and to avoid unnecessary questions that identify protected traits. See the EEOC's National Origin Discrimination guidance and its Title VII of the Civil Rights Act of 1964 resource.

QUESTION NO: 26

A health plan is responding to a member's request for an accounting of disclosures of protected health information. Which disclosure generally does NOT need to be included in the accounting under HIPAA?

A. A disclosure to a public health authority as required by law

B. A disclosure to a law enforcement official pursuant to a legal process

C. A disclosure for treatment, payment, or health care operations

D. A disclosure to a coroner for identifying a deceased individual

ANSWER: C

Explanation:

A disclosure made for treatment, payment, or health care operations generally does not need to be included in an accounting of disclosures. HIPAA's accounting right gives individuals information about certain disclosures of their protected health information made during the relevant accounting period. However, disclosures for treatment, payment, and health care operations are among the specified exclusions from the accounting requirement.

The exclusion does not mean that these uses and disclosures are unrestricted. They must still comply with the HIPAA Privacy Rule and applicable safeguards. The accounting requirements and exclusions appear at 45 C.F.R. § 164.528.

QUESTION NO: 27

What is the most likely reason that states have adopted their own data breach notification laws?

A. Many states have unique types of businesses that require specific legislation

B. Many lawmakers believe that federal enforcement of current laws has not been effective

C. Many types of organizations are not currently subject to federal laws regarding breaches

D. Many large businesses have intentionally breached the personal information of their customers

ANSWER: C

Explanation:

Many types of organizations are not currently subject to federal laws regarding breaches is correct because the United States has historically lacked a single, comprehensive federal data-breach-notification statute covering all private-sector entities and all categories of personal information. Instead, federal requirements have generally been sector-specific. For example, HIPAA's Breach Notification Rule applies to covered entities and business associates handling protected health information, while other federal regimes apply in more limited contexts. This leaves substantial portions of the economy—such as many retailers, online services, and other businesses handling consumers' personal information—outside a generally applicable federal breach-notification mandate.

States adopted breach-notification laws to address that coverage gap and ensure that affected residents receive notice when specified personal information is acquired, accessed, or disclosed without authorization. California's pioneering breach-notification law, effective in 2003, helped establish the model subsequently adopted in every state, the District of Columbia, and U.S. territories. Although the specific triggers, definitions, deadlines, and content requirements vary by jurisdiction, the core policy purpose is to provide broad consumer notice where federal sectoral law does not supply it. See the California Attorney General's data-breach reporting guidance and the HHS HIPAA Breach Notification Rule overview.

QUESTION NO: 28

SCENARIO Please use the following to answer the next question:

A US-based startup company is selling a new gaming application. One day, the CEO of the company receives an urgent letter from a prominent EU-based retail partner. Triggered by an unresolved complaint lodged by an EU resident, the letter describes an ongoing investigation by a supervisory authority into the retailer's data handling practices.

The complainant accuses the retailer of improperly disclosing her personal data, without consent, to parties in the United States. Further, the complainant accuses the EU-based retailer of failing to respond to her withdrawal of consent and request for erasure of her personal data. Your organization, the US-based startup company, was never informed of this request for erasure by the EU-based retail partner. The supervisory authority investigating the complaint has threatened the suspension of data flows if the parties involved do not cooperate with the investigation. The letter closes with an urgent request:

"Please act immediately by identifying all personal data received from our company."

This is an important partnership. Company executives know that its biggest fans come from Western Europe; and this retailer is primarily responsible for the startup's rapid market penetration.

As the Company's data privacy leader, you are sensitive to the criticality of the relationship with the retailer.

At this stage of the investigation, what should the data privacy leader review first?

A. Available data flow diagrams

B. The text of the original complaint

C. The company's data privacy policies

D. Prevailing regulation on this subject

ANSWER: A

Explanation:

Available data flow diagrams should be reviewed first because the immediate request is to identify every category of personal data the startup received from the EU retailer. A current data-flow diagram, or data map, provides the fastest operational view of where data enters the organization, the systems and vendors that receive or store it, the purposes for which it is used, and the onward transfers that may need to be investigated. This lets the privacy leader promptly establish the scope of the retailer-originated data, preserve relevant information, identify the teams that control affected systems, and determine whether the individual's withdrawal of consent and erasure request can be located and actioned across the environment.

This review also supports a coordinated response to the retailer and supervisory authority. GDPR accountability requires organizations to be able to demonstrate compliant processing, and records of processing activities must describe categories of data subjects and personal data, recipients, and, where applicable, third-country transfers. A well-maintained data map is a practical tool for assembling and validating that information during an urgent investigation. The legal framework is important, but the first response must establish the factual processing and transfer inventory implicated by the request. See GDPR Article 30 at EUR-Lex and the European Commission's record-keeping guidance.