IAPP CIPP-US Mock Exam

Shared by May on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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procedures for purging and destroying outdated dat

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 Third, identify outdated customer information and then develop a process for securely disposing of it.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

What could the company have done differently prior to the breach to reduce their risk?

Options:

A- Implemented a comprehensive policy for accessing customer information.
B- Honored the promise of its privacy policy to acquire information by using an opt-in method.
C- Looked for any persistent threats to security that could compromise the company's network.

D- Communicated requests for changes to users' preferences across the organization and with third parties.

Answer:

A

Explanation:

The scenario suggests that the company lacked adequate rules about access to customer information, which increased the risk of unauthorized access and data breach. Implementing a comprehensive policy for accessing customer information would have helped the company to limit the access to only those who need it for legitimate purposes, and to protect the confidentiality, integrity, and availability of the data. This is also one of the recommendations that Roberta made in her report.Reference:

CIPP/US Practice Questions (Sample Questions), Question 116, Answer A, Explanation A.

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 5, Section 5.2, p. 143.

Question 2

Question Type: MultipleChoice

A covered entity suffers a ransomware attack that affects the personal health information (PHI) of more than 500 individuals. Based on Federal law under HIPAA, Which option best would the covered entity NOT have to report the breach to?

Options:

A- Department of Health and Human Services
B- The affected individuals
C- The local media
D- Medical providers

Answer:

D

Explanation:

According to the Health Insurance Portability and Accountability Act (HIPAA), a covered entity is a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA. A covered entity must report a breach of unsecured protected health information (PHI) to the following parties:

The Department of Health and Human Services (HHS), which is the federal agency responsible for enforcing HIPAA and issuing regulations and guidance on privacy and security issues. A covered entity must notify HHS of a breach affecting 500 or more individuals without unreasonable delay and in no case later than 60 days after discovery of the breach. A covered entity must also notify HHS of breaches affecting fewer than 500 individuals within 60 days of the end of the calendar year in which the breaches occurred.

The affected individuals, who are the individuals whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach. A covered entity must notify the affected individuals without unreasonable delay and in no case later than 60 days after discovery of the breach. The notification must be in writing by first-class mail or, if the individual agrees, by electronic mail. The notification must include a brief description of the breach, the types of information involved, the steps the individual should take to protect themselves, the steps the covered entity is taking to investigate and mitigate the breach, and the contact information of the covered entity.

The local media, if the breach affects more than 500 residents of a state or jurisdiction. A covered entity must notify prominent media outlets serving the state or jurisdiction without unreasonable delay and in no case later than 60 days after discovery of the breach. The notification must include the same information as the notification to the affected individuals.

A covered entity does not have to report the breach to medical providers, unless they are also affected individuals or business associates of the covered entity. A business associate is a person or entity that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of PHI. A covered entity must have a written contract or agreement with its business associates that requires them to protect the privacy and security of PHI and report any breaches to the covered entity.

IAPP CIPP/US Body of Knowledge, Domain II: Limits on Private-sector Collection and Use of Data, Section C: Sector-specific Requirements for Health Information

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 2: Limits on Private-sector Collection and Use of Data, Section 2.3: Sector-specific Requirements for Health Information

Practice Exam - International Association of Privacy Professionals

Question 3

Question Type: MultipleChoice

Which statute is considered part of U.S. federal privacy law?

Options:

A- The Fair Credit Reporting Act.
B- SB 1386.
C- The Personal Information Protection and Electronic Documents Act.
D- The e-Privacy Directive.

Answer:

A

Explanation:

The Fair Credit Reporting Act (FCRA) is considered part of U.S. federal privacy law because it regulates the collection, use, and disclosure of personal information by consumer reporting agencies, such as credit bureaus, background check companies, and tenant screening services. The FCRA aims to protect the privacy, accuracy, and fairness of consumer credit information, and to ensure that consumers have access to and control over their own credit reports. The FCRA also imposes obligations on users and furnishers of consumer reports, such as creditors, employers, insurers, and landlords, to obtain consent, provide notice, and correct errors when using consumer reports for various purposes. The FCRA is enforced by the Federal Trade Commission (FTC) and other federal agencies, as well as by private lawsuits and state attorneys general. The FCRA was enacted in 1970 and has been amended several times, most notably by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which added provisions on identity theft prevention, fraud alerts, free credit reports, and disposal of consumer information.Reference:

Fair Credit Reporting Act - Wikipedia

Fair Credit Reporting Act | Federal Trade Commission

Fair Credit Reporting Act (FCRA) - Consumer Information

Fair Credit Reporting Act (FCRA) | Privacy Rights Clearinghouse

Question 4

Question Type: MultipleChoice

Your company, an online store selling digital keys to video games, has received a data access request from an individual. Specifically, the individual wants access to her recent purchase history, as she has misplaced the emails containing the digital keys to multiple game purchases she made last month.

From a security standpoint, what would the user have to do under CCPA in order to acceptably verify her identity?

Options:

A- Take a photo of herself with her driver license
B- Provide a notarized affidavit signed by two witnesses.
C- Log in to her password-protected account with the company
D- Phone the company and provide her contact details and credit card number

Answer:

C

Explanation:

Under the California Consumer Privacy Act (CCPA), businesses must verify the identity of individuals making data access requests to ensure the security of personal information. The most secure and straightforward way to verify a consumer's identity is by requiring the individual to log in to their password-protected account, as this demonstrates that the requester is the account owner.

Why Password-Protected Accounts Are Best for Verification:

Account-Based Relationship: If the consumer has a password-protected account with the business, verification can typically be achieved by having the consumer log in to the account. This is considered a sufficient method of verifying identity under CCPA guidelines.

Minimizing Risk: Verifying identity through account login reduces the risk of fraudulent access to personal information, as only the account owner has access to the login credentials.

Explanation of Options:

A. Take a photo of herself with her driver license: While this might verify identity, it is more intrusive and poses unnecessary risks of identity theft. This is not a preferred or common method under the CCPA.

B. Provide a notarized affidavit signed by two witnesses: This is excessive and impractical for verifying identity in most cases, particularly for an online store.

C. Log in to her password-protected account with the company: This is correct. Logging into a password-protected account is a straightforward and secure way to verify the identity of a requester under the CCPA.

D. Phone the company and provide her contact details and credit card number: This method is insecure, as it could lead to identity theft or fraudulent access if someone else provides this information.

Reference from CIPP/US Materials:

CCPA Regulations (11 CCR 999.323): Specifies identity verification requirements, including the use of password-protected accounts.

IAPP CIPP/US Certification Textbook: Covers secure methods for verifying consumer identity under the CCPA.

Question 5

Question Type: MultipleChoice

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?

Options:

A- Mandatory
B- Implied consent
C- Opt-in
D- Opt-out

Answer:

B

Explanation:

A cookie is a small piece of data that a website sends to a user's browser and stores on the user's device, usually for the purpose of remembering the user's preferences, settings, or actions1.

A cookie notice is a message that informs the user about the website's use of cookies and the user's choices regarding the acceptance or rejection of cookies2.

A legal choice is the mechanism that the website provides to the user to express their consent or dissent to the use of cookies2.

There are different types of legal choices for cookie notices, depending on the applicable laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA) in the United States34.

The four types of legal choices mentioned in the question are:

Mandatory: The website does not allow the user to access the site unless they accept the use of cookies.This type of choice is generally considered unlawful and non-compliant with the GDPR and the CCPA34.

Implied consent: The website assumes that the user consents to the use of cookies by continuing to browse the site or by dismissing the cookie notice. This type of choice is often used by websites that operate in the U.S.or other jurisdictions that do not have strict cookie laws, but it may not be sufficient for the GDPR or the CCPA34.

Opt-in: The website requires the user to explicitly agree to the use of cookies by clicking a button or checking a box.This type of choice is usually compliant with the GDPR and the CCPA, as it ensures that the user gives informed and affirmative consent34.

Opt-out: The website allows the user to reject the use of cookies by clicking a link or changing their browser settings.This type of choice is also compliant with the GDPR and the CCPA, as it gives the user the right to withdraw their consent at any time34.

Based on the description of the cookie notice in the question, the type of legal choice that the notice provides isimplied consent, as the website does not explicitly ask for the user's agreement, but rather assumes that the user accepts the use of cookies by using the site. The notice also provides a link for the user to opt out of cookies by setting their browser to refuse them.

Question 6

Question Type: MultipleChoice

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

Under Section 702 of F1S

Options:

A- the NSA may do which of the following without a Foreign Intelligence Surveillance Court warrant?
A- Compel AWS to disclose Jane's email communications with a Taiwanese national residing in Taiwan.
B- Compel AWS to disclose email communications between two Chinese nationals residing in the EU.
C- Compel Microsoft to disclose Patnck's Skype calls with a Brazilian national living in Peru.
D- Compel Jane to disclose the PIN code for her corporate mobile phone.

Answer:

B

Explanation:

Under Section 702 of the Foreign Intelligence Surveillance Act (FISA), the National Security Agency (NSA) is authorized to collect and analyze communications of non-U.S. persons located outside the United States for foreign intelligence purposes. Section 702 allows the NSA to compel U.S.-based service providers, such as AWS or Microsoft, to provide access to data without requiring a warrant from the Foreign Intelligence Surveillance Court (FISC) if certain criteria are met.

Key Aspects of Section 702:

Scope of Surveillance: Section 702 applies to non-U.S. persons located outside the United States. It cannot be used to target U.S. citizens or individuals located within the United States, even if they communicate with non-U.S. persons.

Provider Obligations: The NSA can compel U.S.-based service providers (e.g., AWS, Microsoft) to disclose information about communications involving foreign individuals if the data is relevant to foreign intelligence purposes.

Explanation of the Options:

A. Compel AWS to disclose Jane's email communications with a Taiwanese national residing in Taiwan: Incorrect. Jane is a U.S. citizen, and Section 702 cannot be used to directly target U.S. persons or their communications, even if the other party in the communication is a non-U.S. person.

B. Compel AWS to disclose email communications between two Chinese nationals residing in the EU: Correct. Section 702 allows the NSA to target non-U.S. persons located outside the U.S. without a warrant, even if their communications are hosted by a U.S.-based service provider like AWS. This scenario falls directly under the scope of Section 702.

C. Compel Microsoft to disclose Patrick's Skype calls with a Brazilian national living in Peru: Incorrect. Patrick is a U.S. resident, even though he is a French citizen. Section 702 cannot be used to target individuals who are lawfully residing in the United States.

D. Compel Jane to disclose the PIN code for her corporate mobile phone: Incorrect. Section 702 applies to electronic communications data held by service providers, not to individuals. Compelling an individual to disclose a PIN code would require a different legal authority, such as a court-issued subpoena or warrant.

Legal Framework:

Section 702 of FISA: Provides the NSA with the authority to compel U.S.-based service providers to assist in collecting data on non-U.S. persons located outside the U.S. for foreign intelligence purposes.

Targeting Limitations: Section 702 cannot be used to intentionally target U.S. persons or anyone located within the United States.

Service Providers: Examples include U.S.-based companies such as Amazon AWS, Microsoft, and Google.

Practical Considerations for Jones Labs:

Jones Labs should be aware that:

Data stored with U.S.-based providers (even if located in the EU) may still be subject to Section 702 requests.

International data transfer compliance may require careful consideration of Standard Contractual Clauses (SCCs) or other safeguards to align with EU privacy regulations, such as the GDPR, in light of the extraterritorial nature of U.S. surveillance laws.

Reference from CIPP/US Materials:

FISA Section 702 (50 U.S.C. 1881a): Outlines the legal authority for targeting non-U.S. persons located outside the United States.

IAPP CIPP/US Certification Textbook: Discusses Section 702 and its implications for U.S.-based service providers handling international data.

Schrems II Decision: Highlights conflicts between U.S. surveillance laws and EU privacy laws, particularly for data stored by U.S. companies overseas.

Question 7

Question Type: MultipleChoice

Mega Corp. is a U.S.-based business with employees in California, Virginia, and Colorado. Which of the following must Mega Corp. comply with in regard to its human resources data?

Options:

A- California Privacy Rights Act.
B- California Privacy Rights Act and Virginia Consumer Data Protection Act.
C- California Privacy Rights Act and Colorado Privacy Act.
D- California Privacy Rights Act, Virginia Consumer Data Protection Act, and Colorado Privacy Act.

Answer:

D

Explanation:

Mega Corp. is a U.S.-based business with employees in California, Virginia, and Colorado.

Therefore, it must comply with the privacy laws of these three states in regard to its human resources data, unless it qualifies for an exemption under each law.

The California Privacy Rights Act (CPRA) is an amendment to the California Consumer Privacy Act (CCPA) that was approved by voters in November 2020 and will take effect on January 1, 2023. The CPRA expands the rights and protections of California residents with respect to their personal information and creates a new category of sensitive personal information that includes certain employment-related data, such as Social Security numbers, driver's license numbers, passport numbers, financial account information, biometric information, and geolocation data. The CPRA also establishes a new enforcement agency, the California Privacy Protection Agency, to oversee and enforce the law.

The Virginia Consumer Data Protection Act (VCDPA) is a comprehensive privacy law that was enacted in March 2021 and will take effect on January 1, 2023. The VCDPA grants Virginia residents several rights with respect to their personal data, such as the right to access, correct, delete, port, and opt out of certain processing activities. The VCDPA also imposes various obligations on businesses that control or process personal data of Virginia residents, such as conducting data protection assessments, entering into contracts with processors, and providing privacy notices.

The Colorado Privacy Act (CPA) is another comprehensive privacy law that was enacted in July 2021 and will take effect on July 1, 2023. The CPA grants Colorado residents similar rights as the VCDPA, with some variations, such as the right to appeal a business's response to a request and the right to opt out of targeted advertising, the sale of personal data, and certain profiling activities. The CPA also imposes similar obligations as the VCDPA, with some differences, such as requiring opt-in consent for the processing of sensitive data and allowing businesses to join a universal opt-out mechanism.

All three laws apply to businesses that conduct business in or target consumers in the respective states and meet certain thresholds of revenue or data processing volume. However, all three laws also provide exemptions for certain types of data or entities that are subject to other federal or state laws, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Family Educational Rights and Privacy Act (FERPA).

One of the exemptions that may be relevant for Mega Corp. is the employee data exemption, which excludes personal data that is collected and used by an employer within the context of an employment relationship or for emergency contact or benefits administration purposes. However, this exemption is not permanent or uniform across the three laws. The CPRA's employee data exemption is set to expire on January 1, 2023, unless extended by the legislature. The VCDPA's employee data exemption is set to expire on January 1, 2023, unless repealed by the legislature. The CPA's employee data exemption does not have an expiration date, but it does not apply to the right to opt out of the sale of personal data or the right to appeal a business's response to a request.

Therefore, depending on the type and scope of the human resources data that Mega Corp. collects and processes, it may have to comply with the California Privacy Rights Act, the Virginia

Consumer Data Protection Act, and the Colorado Privacy Act, unless it qualifies for another exemption under each law.

[IAPP CIPP/US Study Guide], Chapter 10: State Data Security Laws, pp. 227-229.

CIPP/US Practice Questions (Sample Questions), Question 32.

Question 8

Question Type: MultipleChoice

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 CPR

Options:

A- 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, A

Explanation:

Under the California Privacy Rights Act (CPRA), which amends the California Consumer Privacy Act (CCPA), California residents have the right to request access to their personal information collected by a business. However, the CPRA provides an exception for inferences made about an individual for internal purposes, meaning businesses are not obligated to disclose inferences generated solely for internal use.

Key Points Under the CPRA:

Access to Personal Information:

Businesses must provide consumers with access to personal information they have collected,

which includes data submitted by the consumer and other information directly associated with the consumer.

Exception for Inferences:

Inferences made about a consumer, particularly when used for internal purposes (e.g., improving services, analytics, or predicting preferences), are not explicitly required to be disclosed under the CPRA unless they are part of the consumer's profile or used for decision-making purposes that affect the consumer.

Examples of Data to Be Provided:

Information provided by the consumer (e.g., email address, account information).

Automatically collected information (e.g., timestamps, purchase history).

Identifiers (e.g., loyalty account numbers).

Explanation of Options:

A . Inferences made about the individual for the company's internal purposes: This is correct. Inferences generated for internal use are not considered part of the data set that must be disclosed in response to a CPRA data access request.

B . The loyalty account number assigned through the individual's use of the services: Loyalty account numbers are directly associated with the consumer and must be provided in response to an access request under the CPRA.

C. The time stamp for the creation of the individual's account in the platform's database: This information is part of the consumer's account data and must be disclosed under the CPRA.

D . The email address submitted by the individual as part of the account registration process: This is personal information directly provided by the consumer and must be disclosed under the CPRA.

Reference from CIPP/US Materials:

CPRA (Civil Code 1798.140): Defines personal information and exceptions for internal use, including inferences.

IAPP CIPP/US Certification Textbook: Discusses consumer rights under the CPRA, including access rights and the treatment of inferences.

Question 9

Question Type: MultipleChoice

What role does the U.S. Constitution play in the area of workplace privacy?

Options:

A- It provides enforcement resources to large employers, but not to small businesses
B- It provides legal precedent for physical information security, but not for electronic security
C- It provides contractual protections to members of labor unions, but not to employees at will
D- It provides significant protections to federal and state governments, but not to private-sector employment

Answer:

D

Explanation:

The U.S. Constitution plays a limited role in the area of workplace privacy, because it mainly applies to the actions of the government, not private employers.The Fourth Amendment protects the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures1.The Supreme Court has interpreted this right to include a reasonable expectation of privacy in certain situations, such as in one's home, car, or personal belongings2.However, this right does not extend to private-sector employees, who are not protected by the Constitution from the actions of their employers, unless the employer is acting as an agent of the government3.Private-sector employees may have some privacy rights under state laws, common law, or contractual agreements, but these vary depending on the jurisdiction and the circumstances4.

Public-sector employees, on the other hand, are protected by the Constitution from unreasonable searches and seizures by their employers, who are considered part of the government. Public-sector employees have a reasonable expectation of privacy in their workplace, unless there is a legitimate work-related reason for the search or seizure, such as to ensure safety, security, or efficiency. Public-sector employers must also comply with the due process and equal protection clauses of the Fifth and Fourteenth Amendments, which prohibit the government from depriving any person of life, liberty, or property without due process of law, or from denying any person the equal protection of the laws. These clauses protect public-sector employees from arbitrary or discriminatory actions by their employers that affect their employment status or benefits.

Therefore, the U.S. Constitution plays a significant role in the area of workplace privacy for federal and state governments, but not for private-sector employment, because it only regulates the actions of the government, not private actors.Reference:

1: Cornell Law School, Fourth Amendment, https://www.law.cornell.edu/constitution/fourth_amendment

2: FindLaw, What Is a Reasonable Expectation of Privacy?, https://www.findlaw.com/criminal/criminal-rights/what-is-a-reasonable-expectation-of-privacy.html

3: FindLaw, Workplace Privacy, https://www.findlaw.com/smallbusiness/employment-law-and-human-resources/workplace-privacy.html

4: Nolo, Privacy Rights of Employees, https://www.nolo.com/legal-encyclopedia/privacy-rights-employees-29849.html

: OPM, Employee Relations, https://www.opm.gov/policy-data-oversight/employee-relations/reference-materials/employee-privacy/

: Cornell Law School, Fifth Amendment, https://www.law.cornell.edu/constitution/fifth_amendment

: FindLaw, Public Employees and the Constitution, https://www.findlaw.com/employment/employment-rights/public-employees-and-the-constitution.html

Question 10

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next question;

Miraculous Healthcare is a large medical practice with multiple locations in California and Nevad

a. Miraculous normally treats patients in person, but has recently decided to start offering teleheaith 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 MedApps

What is the most practical action Riya can take to minimize the privacy risks of using an app for telehealth appointments?

Options:

A- Prevent MedApps from using copies of the patient data.
B- Require MedApps to obtain consent from all patients.
C- Require MedApps to submit a SOC2 report.
D- Engage in active oversight of MedApps

Answer:

D

Explanation:

When handling sensitive data, such as protected health information (PHI) in compliance with HIPAA, it is crucial for covered entities, such as Miraculous Healthcare, to ensure that their business associates (e.g., MedApps) appropriately safeguard the data they process. While contracts like Business Associate Agreements (BAAs) establish the obligations of business associates, active oversight by the covered entity is a practical and necessary step to mitigate privacy risks and ensure compliance.

Why Active Oversight is the Best Option:

Active oversight involves regular monitoring, audits, and reviews of MedApps' practices to ensure they comply with the agreed-upon privacy and security obligations.

This approach allows Miraculous Healthcare to confirm that MedApps is implementing appropriate technical and organizational safeguards, such as encryption, secure access controls, and breach notification processes.

It also ensures that MedApps remains compliant with HIPAA requirements over time, even if there are changes to the app, its services, or legal requirements.

Explanation of Options:

A. Prevent MedApps from using copies of the patient data: While restricting MedApps from creating unnecessary data copies could reduce some risks, it is often impractical, especially for troubleshooting, app hosting, and support purposes. HIPAA does not require outright prevention of data copies, as long as PHI is appropriately safeguarded and used solely for permissible

purposes.

B. Require MedApps to obtain consent from all patients: Under HIPAA, covered entities (not business associates) are primarily responsible for obtaining patient consent or authorization where required. MedApps, as a business associate, processes PHI on behalf of Miraculous Healthcare and is not in a position to obtain consent directly from patients.

C. Require MedApps to submit a SOC2 report: A SOC 2 (Service Organization Control 2) report can provide valuable assurance regarding MedApps' security, availability, and confidentiality practices. However, this action alone does not mitigate all risks, as SOC 2 reports are point-in-time assessments and may not reflect ongoing compliance or address specific HIPAA requirements.

D. Engage in active oversight of MedApps: This is the most practical and comprehensive approach. Active oversight includes reviewing MedApps' privacy practices, conducting periodic assessments, and monitoring compliance with the Business Associate Agreement (BAA). It ensures that MedApps continues to protect PHI appropriately and addresses any privacy risks proactively.

Additional Context:

In the context of the optional benchmarking service, Riya should ensure:

The uploaded data is de-identified or aggregated to comply with HIPAA's de-identification standard (45 CFR 164.514) if possible.

The use of PHI for benchmarking is explicitly addressed in the BAA or a separate agreement.

Reference from CIPP/US Materials:

HIPAA Privacy Rule (45 CFR 160.103 and 164.504): Describes the responsibilities of covered entities and business associates, including the need for BAAs and safeguards for PHI.

NIST Privacy Framework and NIST SP 800-53: Provides guidance on implementing oversight mechanisms for third-party risk management.

IAPP CIPP/US Certification Textbook: Discusses the importance of vendor management and active oversight in ensuring privacy compliance.

Conclusion:

Requiring MedApps to submit a SOC 2 report or restricting data use might address specific concerns but would not provide the comprehensive, ongoing protection necessary to reduce risks effectively. Engaging in active oversight is the most practical and effective action to minimize privacy risks while maintaining compliance with HIPAA.

Question 11

Question Type: MultipleChoice

Under the EU-US Data Privacy Framework, what must participating organizations provide to individuals in regard to complaints and disputes?

Options:

A- An independent recourse mechanism.
B- A copy 01 the individual's personal data
C- A description of the organization's data processing policies
D- A means of communicating with the organization's privacy team.
D- A means of communicating with the organization's privacy team: While communication channels are essential, they do not meet the requirement for an independent recourse mechanism as stipulated by the DPF.
Reference from CIPP/US Materials:
EU-US Data Privacy Framework Principles: Specifically, the 'Recourse, Enforcement, and Liability' principle requires participating organizations to provide an independent recourse mechanism for complaints.
IAPP CIPP/US Certification Textbook: Discusses dispute resolution and redress mechanisms as a cornerstone of international data transfer agreements.
US Department of Commerce Privacy Shield Program Website: Similar requirements under the now-replaced Privacy Shield have been carried over to the DPF, ensuring individuals have access to independent redress mechanisms.

Answer:

A

Explanation:

Under the EU-US Data Privacy Framework (DPF), organizations that participate in the framework must provide individuals with a way to resolve complaints and disputes about how their personal data is handled. Specifically, organizations are required to offer an independent recourse mechanism to ensure compliance with the principles of the framework. This mechanism enables individuals to bring their complaints forward and have them addressed through an impartial and accessible process.

The independent recourse mechanism is critical to the DPF as it reinforces accountability and builds trust in cross-border data transfers. Organizations must select a third-party dispute resolution provider (such as an alternative dispute resolution body or a regulatory body) and disclose this mechanism in their privacy policies. The mechanism must be provided free of

charge to the individual.

Explanation of Options:

A . An independent recourse mechanism: This is the correct answer, as it is explicitly required under the EU-US Data Privacy Framework for resolving disputes and complaints related to data privacy.

B . A copy of the individual's personal data: While data access rights are part of broader privacy regulations (e.g., GDPR), this is not specific to the EU-US DPF's requirements regarding complaint handling.

C . A description of the organization's data processing policies: While transparency about data processing is an important requirement under the DPF, it does not address the need for a formal dispute resolution mechanism.

P2P exams