Vendor: IAPP

Exam Code: CIPP-US

Exam Name: Certified Information Privacy Professional/United States (CIPP/US)

Version: DEMO

QUESTION 1
In which situation would a policy of "no consumer choice" or "no option" be expected?

A. When a job applicant's credit report is provided to an employer
B. When a customer's financial information is requested by the government
C. When a patient's health record is made available to a pharmaceutical company
D. When a customer's street address is shared with a shipping company

Answer: B
Explanation:
According to the Family Educational Rights and Privacy Act (FERPA), a policy of "no consumer choice" or "no option" means that an educational agency or institution may disclose personally identifiable information (PII) from education records without the prior written consent of the parent or eligible student, subject to certain conditions and exceptions. One of the exceptions is when the disclosure is to comply with a judicial order or lawfully issued subpoena, or to respond to an ex parte order from the Attorney General of the United States or his designee in connection with the investigation or prosecution of terrorism crimes. In such cases, the educational agency or institution must make a reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance, unless the order or subpoena specifies not to do so. Therefore, when a customer's financial information, which may be part of the education records, is requested by the government under a valid legal authority, the customer does not have the option to prevent the disclosure and the educational agency or institution does not need to obtain the customer's consent.

QUESTION 2
What is the main challenge financial institutions face when managing user preferences?

A. Ensuring they are in compliance with numerous complex state and federal privacy laws
B. Developing a mechanism for opting out that is easy for their consumers to navigate
C. Ensuring that preferences are applied consistently across channels and platforms
D. Determining the legal requirements for sharing preferences with their affiliates

Answer: C
Explanation:
Financial institutions (FIs) collect and process a large amount of personal data from their customers, such as name, address, account number, transaction history, credit score, etc. Customers may have different preferences regarding how their data is used, shared, or protected by the FIs. For example, some customers may want to receive marketing offers from the FIs or their affiliates, while others may opt out of such communications. Some customers may prefer to access their accounts online, while others may use mobile apps, phone calls, or physical branches. Some customers may want to enable biometric authentication, while others may rely on passwords or PINs. Managing these diverse and dynamic user preferences is a challenge for FIs, as they need to ensure that they respect and honor the choices of their customers across all the channels and platforms they use. This requires FIs to have a robust and integrated system that can capture, store, update, and apply user preferences consistently and accurately. Failing to do so may result in customer dissatisfaction, loss of trust, regulatory fines, or legal disputes.

QUESTION 3
A large online bookseller decides to contract with a vendor to manage Personal Information (PI). What is the least important factor for the company to consider when selecting the vendor?

A. The vendor's reputation

B. The vendor's financial health
C. The vendor's employee retention rates
D. The vendor's employee training program

Answer: C
Explanation:
When selecting a vendor to manage personal information, the company should consider various criteria, such as the vendor's reputation, financial health, employee training program, privacy policies, security practices, compliance record, contractual terms, and service quality. However, the vendor's employee retention rates may not be as important as the other factors, as they do not directly affect the vendor's ability to protect and process the personal information entrusted to them. While high employee turnover may indicate some issues with the vendor's management or culture, it may not necessarily impact the vendor's performance or reliability, as long as the vendor has adequate measures to ensure continuity, accountability, and confidentiality of the personal information they handle.

QUESTION 4
SCENARIO

Please use the following to answer the next question:

Matt went into his son's bedroom one evening and found him stretched out on his bed typing on his laptop. "Doing your network?" Matt asked hopefully.
"No," the boy said. "I'm filling out a survey."

Matt looked over his son's shoulder at his computer screen. "What kind of survey?" "It's asking Questions about my opinions."
"Let me see," Matt said, and began reading the list of Questions that his son had already answered. "It's asking your opinions about the government and citizenship. That's a little odd. You're only ten."

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

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

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

How could the marketer have best changed its privacy management program to meet COPPA "Safe Harbor" requirements?

A. By receiving FTC approval for the content of its emails
B. By making a COPPA privacy notice available on website
C. By participating in an approved self-regulatory program
D. By regularly assessing the security risks to consumer privacy

Answer: C
Explanation:
The Children's Online Privacy Protection Act (COPPA) is a federal law that protects the privacy of children under 13 who use online sites and services. COPPA requires operators of such sites and services to obtain verifiable parental consent before collecting, using, or disclosing personal information from children, and to provide notice of their information practices to parents and the public. COPPA also gives parents the right to access, review, and delete their children's personal information, and to limit further collection or use of such information. One way for operators to comply with COPPA is to participate in an approved self-regulatory program, also known as a "safe harbor" program. These are programs that are run by industry groups or other organizations that set and enforce standards for privacy protection that meet or exceed the requirements of COPPA. Operators that join a safe harbor program and follow its guidelines are deemed to be in compliance with COPPA and are subject to the review and disciplinary procedures of the program instead of FTC enforcement actions. The FTC has approved several safe harbor programs, such as CARU, ESRB, iKeepSafe, kidSAFE, PRIVO, and TRUSTe. By participating in an approved self-regulatory program, the marketer in the scenario could have best changed its privacy management program to meet COPPA "Safe Harbor" requirements. This would mean that the marketer would have to adhere to the guidelines of the program, which would likely include obtaining verifiable parental consent before collecting personal information from children, providing clear and prominent privacy notices on its website and emails, honoring parents' choices and requests regarding their children's data, and ensuring the security and confidentiality of the data collected. The marketer would also benefit from the oversight and assistance of the program in ensuring compliance and resolving any complaints or disputes.

QUESTION 5
What important action should a health care provider take if the she wants to qualify for funds under the Health Information Technology for Economic and Clinical Health Act (HITECH)?

A. Make electronic health records (EHRs) part of regular care
B. Bill the majority of patients electronically for their health care
C. Send health information and appointment reminders to patients electronically
D. Keep electronic updates about the Health Insurance Portability and Accountability Act

Answer: A
Explanation:
The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009 to promote the adoption and use of health information technology, especially electronic health records (EHRs), in the United States. The HITECH Act established the Medicare and Medicaid EHR Incentive Programs, which provide financial incentives to eligible health care providers who demonstrate meaningful use of certified EHR technology. Meaningful use is defined as using EHRs to improve quality, safety, efficiency, and coordination of care, as well as to engage patients and protect their privacy and security. To qualify for the incentive payments, health care providers must meet certain objectives and measures that demonstrate meaningful use of EHRs as part of their regular care.

QUESTION 6
All of the following organizations are specified as covered entities under the Health Insurance Portability and Accountability Act (HIPAA) EXCEPT?

A. Healthcare information clearinghouses
B. Pharmaceutical companies
C. Healthcare providers

D. Health plans

Answer: C
Explanation:
The Privacy Act of 1974 is a federal law that regulates the collection, use, and disclosure of personal information by federal agencies.
The Privacy Act of 1974 applies to records that are maintained in a system of records, which is defined as a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.
The Privacy Act of 1974 grants individuals the right to access and amend their records, and requires agencies to provide notice of their systems of records, establish safeguards for the protection of the records, and limit the disclosure of the records to certain authorized purposes.
The Privacy Act of 1974 also establishes civil and criminal penalties for violations of the law, such as unauthorized disclosure, failure to publish a notice, or refusal to grant access or amendment.
The Privacy Act of 1974 does NOT require agencies to obtain the consent of the individual before collecting their personal information. However, the Privacy Act of 1974 does require agencies to inform the individual of the authority for the collection, the purpose and use of the collection, and the effects of not providing the information.

QUESTION 7
A covered entity suffers a ransomware attack that affects the personal health information (PHI) of more than 500 individuals. According to Federal law under HIPAA, which of the following would the covered entity NOT have to report the breach to?

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.

QUESTION 8
What consumer protection did the Fair and Accurate Credit Transactions Act (FACTA) require?

A. The ability for the consumer to correct inaccurate credit report information
B. The truncation of account numbers on credit card receipts
C. The right to request removal from e-mail lists
D. Consumer notice when third-party data is used to make an adverse decision

Answer: B
Explanation:
The Fair and Accurate Credit Transactions Act (FACTA) is an amendment to the Fair Credit Reporting Act (FCRA) that was enacted in 200. FACTA aims to enhance consumer protection against identity theft and fraud by requiring various measures, such as free annual credit reports, fraud alerts, and identity theft prevention programs. One of the consumer protections that FACTA requires is the truncation of account numbers on credit card receipts. This means that only the last four or five digits of the account number can be printed on the receipt, while the rest must be masked or deleted. This reduces the risk of unauthorized access or use of the account number by third parties who may obtain the receipt.

QUESTION 9
Who has rulemaking authority for the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA)?

A. State Attorneys General
B. The Federal Trade Commission
C. The Department of Commerce
D. The Consumer Financial Protection Bureau

Answer: D
Explanation:
The Consumer Financial Protection Bureau (CFPB) has rulemaking authority for the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA), as well as other consumer financial laws. The Dodd-Frank Act, enacted in 2010, transferred most of the rulemaking responsibilities added to the FCRA by the FACTA and the Credit CARD Act from the Federal Trade Commission (FTC) to the CFPB. However, the FTC retains its enforcement authority for the FCRA and the FACTA, along with other federal and state agencies. The CFPB also shares rulemaking authority for some provisions of the FACTA with the FTC, such as the identity theft red flags and address discrepancy rules. The Department of Commerce and the State Attorneys General do not have rulemaking authority for the FCRA or the FACTA.

QUESTION 10
Under the Fair and Accurate Credit Transactions Act (FACTA), what is the most appropriate action for a car dealer holding a paper folder of customer credit reports?

A. To follow the Disposal Rule by having the reports shredded
B. To follow the Red Flags Rule by mailing the reports to customers
C. To follow the Privacy Rule by notifying customers that the reports are being stored
D. To follow the Safeguards Rule by transferring the reports to a secure electronic file

Answer: A
Explanation:
The Disposal Rule is a provision of the Fair and Accurate Credit Transactions Act (FACTA) that requires businesses and individuals to take appropriate measures to dispose of sensitive information about consumers, such as credit reports, that are derived from consumer reports. The Disposal Rule is intended to reduce the risk of identity theft and fraud by preventing unauthorized access to or use of the information. According to the Disposal Rule, reasonable steps for disposal include burning, pulverizing, or shredding papers that contain consumer report information so that they cannot be read or reconstructed.
In this scenario, the most appropriate action for a car dealer holding a paper folder of customer credit reports is to follow the Disposal Rule by having the reports shredded. This would ensure that the car dealer complies with the FACTA and protects the privacy and security of the customers' personal data.

QUESTION 11
When may a financial institution share consumer information with non-affiliated third parties for marketing purposes?

A. After disclosing information-sharing practices to customers and after giving them an opportunity to opt in.
B. After disclosing marketing practices to customers and after giving them an opportunity to opt in.
C. After disclosing information-sharing practices to customers and after giving them an opportunity to opt out.
D. After disclosing marketing practices to customers and after giving them an opportunity to opt out.

Answer: C
Explanation:
According to the Gramm-Leach-Bliley Act (GLBA) and its implementing Regulation P, a financial institution may share consumer information with non-affiliated third parties for marketing purposes only after disclosing its information-sharing practices to customers and after giving them an opportunity to opt out of such sharing. The GLBA defines a customer as a consumer who has a continuing relationship with a financial institution that provides one or more financial products or services to be used primarily for personal, family, or household purposes. A consumer is an individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative. A non-affiliated third party is any person except a financial institution's affiliate or a person employed jointly by a financial institution and a company that is not the financial institution's affiliate. An affiliate is any company that controls, is controlled by, or is under common control with another company.
The GLBA requires that a financial institution provide a privacy notice to customers: (i) at the time of establishing the customer relationship; (ii) annually during the continuation of the customer relationship; and (iii) before disclosing any nonpublic personal information (NPI) about the customer to any non-affiliated third party, unless an exception applies. The privacy notice must describe the categories of NPI that the financial institution collects and discloses; the categories of affiliates and non-affiliated third parties to whom the financial institution discloses NPI; the categories of NPI disclosed to service providers and joint marketers; the policies and practices with respect to protecting the confidentiality and security of NPI; and the disclosures of NPI to which the customer has a right to opt out. The financial institution must also provide a reasonable means for the customer to opt out of the disclosure of NPI to non-affiliated third parties, such as a

check-off box, a reply form, or a toll-free telephone number. The opt-out notice must be clear and conspicuous, and must state that the customer can opt out at any time. The opt-out notice must also explain how the customer can opt out, and the effect of opting out. The financial institution must honor the customer's opt-out direction as soon as reasonably practicable after receiving it, and must not disclose any NPI to which the opt-out applies, unless an exception applies. The GLBA provides several exceptions to the opt-out requirement, such as when the disclosure of NPI is necessary to effect, administer, or enforce a transaction requested or authorized by the customer; when the disclosure of NPI is required or permitted by law; when the disclosure of NPI is to a consumer reporting agency in accordance with the Fair Credit Reporting Act; or when the disclosure of NPI is to a person that performs marketing services on behalf of the financial institution or on behalf of the financial institution and another financial institution under a joint marketing agreement. A joint marketing agreement is a formal written contract between a financial institution and any other person under which the parties agree to offer, endorse, or sponsor a financial product or service. The joint marketing agreement must prohibit the other person from using or disclosing the NPI for any purpose other than offering, endorsing, or sponsoring the financial product or service covered by the agreement.
The GLBA also requires that a financial institution provide a privacy notice to consumers who are not customers before disclosing any NPI about the consumer to any non-affiliated third party, unless an exception applies. The financial institution does not need to provide an opt-out notice to consumers who are not customers, unless it has a customer relationship with them. However, if the financial institution establishes a customer relationship with a consumer who was previously not a customer, it must provide a privacy notice and an opt-out notice to the customer as described above.

QUESTION 12
What are banks required to do under the Gramm-Leach-Bliley Act (GLBA)?

A. Conduct annual consumer surveys regarding satisfaction with user preferences
B. Process requests for changes to user preferences within a designated time frame
C. Provide consumers with the opportunity to opt out of receiving telemarketing phone calls
D. Offer an Opt-Out before transferring PI to an unaffiliated third party for the latter's own use

Answer: D
Explanation:
The Gramm-Leach-Bliley Act (GLBA) is a federal law that regulates the privacy and security of consumer financial information collected, used, and disclosed by financial institutions, such as banks, credit unions, securities firms, insurance companies, and others. Under the GLBA, financial institutions must comply with two main rules: the Privacy Rule and the Safeguards Rule. The Privacy Rule requires financial institutions to provide notice to their customers about their information-sharing practices and to obtain verifiable parental consent before collecting, using, or disclosing personal information from children. The Privacy Rule also gives customers the right to opt out of having their personal information shared with certain nonaffiliated third parties, unless an exception applies. The Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive information security program that protects the confidentiality, security, and integrity of customer information.
Therefore, banks and other financial institutions are required to offer an opt-out before transferring personal information (PI) to an unaffiliated third party for the latter's own use, unless an exception applies, such as when the disclosure is necessary to complete a transaction requested or authorized by the customer, or when the disclosure is to a service provider or joint marketer that agrees to protect the information and use it only for the purposes for which it was disclosed. This requirement is intended to give customers more control over how their personal information is used and shared by financial institutions and to protect their privacy rights.

QUESTION 13
SCENARIO

Please use the following to answer the next question:

Declan has just started a job as a nursing assistant in a radiology department at Woodland Hospital. He has also started a program to become a registered nurse.

Before taking this career path, Declan was vaguely familiar with the Health Insurance Portability and Accountability Act (HIPAA). He now knows that he must help ensure the security of his patients' Protected Health Information (PHI). Therefore, he is thinking carefully about privacy issues.

On the morning of his first day, Declan noticed that the newly hired receptionist handed each patient a HIPAA privacy notice. He wondered if it was necessary to give these privacy notices to returning patients, and if the radiology department could reduce paper waste through a system of one-time distribution.

He was also curious about the hospital's use of a billing company. He questioned whether the hospital was doing all it could to protect the privacy of its patients if the billing company had details about patients' care.

On his first day Declan became familiar with all areas of the hospital's large radiology department. As he was organizing equipment left in the halfway, he overheard a conversation between two hospital administrators. He was surprised to hear that a portable hard drive containing non-encrypted patient information was missing. The administrators expressed relief that the hospital would be able to avoid liability. Declan was surprised, and wondered whether the hospital had plans to properly report what had happened.

Despite Declan's concern about this issue, he was amazed by the hospital's effort to integrate Electronic Health Records (EHRs) into the everyday care of patients. He thought about the potential for streamlining care even more if they were accessible to all medical facilities nationwide.

Declan had many positive interactions with patients. At the end of his first day, he spoke to one patient, John, whose father had just been diagnosed with a degenerative muscular disease. John was about to get blood work done, and he feared that the blood work could reveal a genetic predisposition to the disease that could affect his ability to obtain insurance coverage. Declan told John that he did not think that was possible, but the patient was wheeled away before he could explain why. John plans to ask a colleague about this.

In one month, Declan has a paper due for one his classes on a health topic of his choice. By then, he will have had many interactions with patients he can use as examples. He will be pleased to give credit to John by name for inspiring him to think more carefully about genetic testing.

Although Declan's day ended with many Questions, he was pleased about his new position.

What is the most likely way that Declan might directly violate the Health Insurance Portability and Accountability Act (HIPAA)?

A. By being present when patients are checking in
B. By speaking to a patient without prior authorization
C. By ignoring the conversation about a potential breach
D. By following through with his plans for his upcoming paper

Answer: D
Explanation:
Declan might directly violate the HIPAA Privacy Rule by using John's name and personal health information (PHI) in his paper without his written authorization. The Privacy Rule protects the confidentiality of PHI that is created, received, maintained, or transmitted by a covered entity or its business associate. PHI includes any information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Declan, as a nursing assistant, is part of the covered entity's workforce and must comply with the Privacy Rule. He cannot disclose John's PHI to anyone, including his classmates or instructors, without John's authorization or a valid exception under the Privacy Rule. Even if he does not use John's full name, he may still reveal enough information to make John identifiable, such as his diagnosis, his father's condition, or his location. This would be an impermissible use and disclosure of PHI, and a potential HIPAA violation. Declan should either obtain John's written authorization to use his PHI in his paper, or de-identify the information according to the Privacy Rule's standards.

QUESTION 14
SCENARIO

Please use the following to answer the next question:

Declan has just started a job as a nursing assistant in a radiology department at Woodland Hospital. He has also started a program to become a registered nurse.

Before taking this career path, Declan was vaguely familiar with the Health Insurance Portability and Accountability Act (HIPAA). He now knows that he must help ensure the security of his patients' Protected Health Information (PHI). Therefore, he is thinking carefully about privacy issues.

On the morning of his first day, Declan noticed that the newly hired receptionist handed each patient a HIPAA privacy notice. He wondered if it was necessary to give these privacy notices to returning patients, and if the radiology department could reduce paper waste through a system of one-time distribution.

He was also curious about the hospital's use of a billing company. He questioned whether the hospital was doing all it could to protect the privacy of its patients if the billing company had details about patients' care.

On his first day Declan became familiar with all areas of the hospital's large radiology department. As he was organizing equipment left in the halfway, he overheard a conversation between two hospital administrators. He was surprised to hear that a portable hard drive containing non-encrypted patient information was missing. The administrators expressed relief that the hospital would be able to avoid liability. Declan was surprised, and wondered whether the hospital had plans to properly report what had happened.

Despite Declan's concern about this issue, he was amazed by the hospital's effort to integrate Electronic Health Records (EHRs) into the everyday care of patients. He thought about the potential for streamlining care even more if they were accessible to all medical facilities nationwide.

Declan had many positive interactions with patients. At the end of his first day, he spoke to one patient, John, whose father had just been diagnosed with a degenerative muscular disease. John

was about to get blood work done, and he feared that the blood work could reveal a genetic predisposition to the disease that could affect his ability to obtain insurance coverage. Declan told John that he did not think that was possible, but the patient was wheeled away before he could explain why. John plans to ask a colleague about this.

In one month, Declan has a paper due for one his classes on a health topic of his choice. By then, he will have had many interactions with patients he can use as examples. He will be pleased to give credit to John by name for inspiring him to think more carefully about genetic testing.

Although Declan's day ended with many Questions, he was pleased about his new position.

How can the radiology department address Declan's concern about paper waste and still comply with the Health Insurance Portability and Accountability Act (HIPAA)?

A. State the privacy policy to the patient verbally
B. Post the privacy notice in a prominent location instead
C. Direct patients to the correct area of the hospital website
D. Confirm that patients are given the privacy notice on their first visit

Answer: D
Explanation:
HIPAA requires covered entities to provide a notice of privacy practices (NPP) to individuals who receive health care services from the covered entity. The NPP must describe how the covered entity may use and disclose protected health information (PHI), the individual's rights with respect to their PHI, and the covered entity's obligations to protect the privacy of PHI. The NPP must be provided to the individual no later than the date of the first service delivery, either in person or electronically. The covered entity must also make the NPP available on request and post it on its website if it has one. The covered entity must also make a good faith effort to obtain a written acknowledgment from the individual that they received the NPP. If the individual refuses to sign the acknowledgment, the covered entity must document the attempt and the reason for the refusal.

QUESTION 15
SCENARIO

Please use the following to answer the next question:

Declan has just started a job as a nursing assistant in a radiology department at Woodland Hospital. He has also started a program to become a registered nurse.

Before taking this career path, Declan was vaguely familiar with the Health Insurance Portability and Accountability Act (HIPAA). He now knows that he must help ensure the security of his patients' Protected Health Information (PHI). Therefore, he is thinking carefully about privacy issues.

On the morning of his first day, Declan noticed that the newly hired receptionist handed each patient a HIPAA privacy notice. He wondered if it was necessary to give these privacy notices to returning patients, and if the radiology department could reduce paper waste through a system of one-time distribution.

He was also curious about the hospital's use of a billing company. He questioned whether the hospital was doing all it could to protect the privacy of its patients if the billing company had details about patients' care.

On his first day Declan became familiar with all areas of the hospital's large radiology department. As he was organizing equipment left in the halfway, he overheard a conversation between two hospital administrators. He was surprised to hear that a portable hard drive containing non-encrypted patient information was missing. The administrators expressed relief that the hospital would be able to avoid liability. Declan was surprised, and wondered whether the hospital had plans to properly report what had happened.

Despite Declan's concern about this issue, he was amazed by the hospital's effort to integrate Electronic Health Records (EHRs) into the everyday care of patients. He thought about the potential for streamlining care even more if they were accessible to all medical facilities nationwide.

Declan had many positive interactions with patients. At the end of his first day, he spoke to one patient, John, whose father had just been diagnosed with a degenerative muscular disease. John was about to get blood work done, and he feared that the blood work could reveal a genetic predisposition to the disease that could affect his ability to obtain insurance coverage. Declan told John that he did not think that was possible, but the patient was wheeled away before he could explain why. John plans to ask a colleague about this.

In one month, Declan has a paper due for one his classes on a health topic of his choice. By then, he will have had many interactions with patients he can use as examples. He will be pleased to give credit to John by name for inspiring him to think more carefully about genetic testing.

Although Declan's day ended with many Questions, he was pleased about his new position.

Based on the scenario, what is the most likely way Declan's supervisor would answer his question about the hospital's use of a billing company?

A. By suggesting that Declan look at the hospital's publicly posted privacy policy
B. By assuring Declan that third parties are prevented from seeing Private Health Information (PHI)
C. By pointing out that contracts are in place to help ensure the observance of minimum security standards
D. By describing how the billing system is integrated into the hospital's electronic health records (EHR) system

Answer: C
Explanation:
HIPAA requires covered entities, such as hospitals, to enter into contracts with their business associates, such as billing companies, that access, use, or disclose protected health information (PHI). These contracts, known as business associate agreements (BAAs), must specify the permitted and required uses and disclosures of PHI by the business associate, as well as the safeguards, reporting, and termination procedures that the business associate must follow to protect the privacy and security of PHI. By having these contracts in place, the hospital can ensure that the billing company is complying with HIPAA and observing the minimum security standards required by law.

QUESTION 16
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 (TSR) is a federal regulation that applies to telemarketing calls, which are defined as "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call." The TSR requires telemarketers to make specific disclosures, prohibit misrepresentations, limit the times and number of calls, and set payment restrictions for the sale of certain goods and services. The TSR also gives consumers the right to opt out of receiving telemarketing calls by registering their phone numbers on the National Do Not Call Registry. The TSR applies to both for-profit and not-for-profit organizations, but there are some exemptions and partial exemptions for certain types of entities, calls, and transactions. For example, the TSR does not apply to nonprofit organizations calling on their own behalf, as they are not considered to be engaged in telemarketing. However, if a nonprofit organization hires a for-profit telemarketer or telefunder to solicit charitable contributions on its behalf, the for-profit entity must comply with the TSR, as it is engaged in telemarketing. Similarly, the TSR does not apply to for-profit organizations calling businesses when a binding contract exists between them, as they are not considered to be inducing the purchase of goods or services. However, if a for-profit organization calls businesses to sell additional services to established customers, the TSR applies, as it is considered to be inducing the purchase of goods or services.
Therefore, among the four options, only for-profit organizations and for-profit telefunders regarding charitable solicitations must comply with the TSR, as they are engaged in telemarketing and do not fall under any of the exemptions or partial exemptions.

QUESTION 17
Under the Telemarketing Sales Rule, what characteristics of consent must be in place for an organization to acquire an exception to the Do-Not-Call rules for a particular consumer?

A. The consent must be in writing, must state the times when calls can be made to the consumer and must be signed
B. The consent must be in writing, must contain the number to which calls can be made and must have an end date
C. The consent must be in writing, must contain the number to which calls can be made and must be signed
D. The consent must be in writing, must have an end data and must state the times when calls can be made

Answer: C
Explanation:
The Telemarketing Sales Rule (TSR) is a federal regulation that applies to telemarketing calls, which are defined as "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call." The TSR requires telemarketers to make specific disclosures, prohibit misrepresentations, limit the times and number of calls, and set payment restrictions for the sale of certain goods and services. The TSR also gives consumers the right to opt out of receiving telemarketing calls by registering their phone numbers on the National Do Not Call Registry. The TSR applies to both for-profit and not-for-profit organizations, but there are some exemptions and partial exemptions for certain types of entities, calls, and transactions. For example, the TSR does not apply to nonprofit organizations calling on their own behalf, as they are not considered to be engaged in telemarketing. However, if a nonprofit organization hires a for-profit telemarketer or telefunder to solicit charitable contributions on its behalf, the for-profit entity must comply with the TSR, as it is engaged in telemarketing. Similarly,

the TSR does not apply to for-profit organizations calling businesses when a binding contract exists between them, as they are not considered to be inducing the purchase of goods or services. However, if a for-profit organization calls businesses to sell additional services to established customers, the TSR applies, as it is considered to be inducing the purchase of goods or services.
Therefore, among the four options, only for-profit organizations and for-profit telefunders regarding charitable solicitations must comply with the TSR, as they are engaged in telemarketing and do not fall under any of the exemptions or partial exemptions.

QUESTION 18
When does the Telemarketing Sales Rule require an entity to share a do-not-call request across its organization?

A. When the operational structures of its divisions are not transparent
B. When the goods and services sold by its divisions are very similar
C. When a call is not the result of an error or other unforeseen cause
D. When the entity manages user preferences through multiple platforms

Answer: A
Explanation:
The Telemarketing Sales Rule (TSR) is a federal regulation that implements the Telemarketing and Consumer Fraud and Abuse Prevention Act of 199. The TSR aims to protect consumers from deceptive or abusive telemarketing practices, such as unwanted calls, false or misleading claims, unauthorized billing, and privacy violations.
The TSR requires telemarketers and sellers to comply with the National Do Not Call Registry, which is a list of phone numbers of consumers who have indicated that they do not want to receive telemarketing calls.
The TSR also requires telemarketers and sellers to honor the do-not-call requests of individual consumers, regardless of whether their numbers are on the National Do Not Call Registry or not. A do-not-call request is a statement made by a consumer, either orally or in writing, that they do not wish to receive any more calls from a specific telemarketer or seller. The TSR requires an entity to share a do-not-call request across its organization when the operational structures of its divisions are not transparent to consumers. This means that the entity must treat the do-not-call request as if it applies to all of its affiliates and subsidiaries that engage in telemarketing, unless the consumer would reasonably expect them to be separate and distinct entities based on their names, products, or services. The TSR does not require an entity to share a do-not-call request across its organization in the following situations:
When the goods and services sold by its divisions are very similar. This is not a relevant factor for determining whether the entity must share a do-not-call request across its organization. The key factor is whether the consumers can distinguish between the different divisions based on their operational structures.
When a call is not the result of an error or other unforeseen cause. This is not an exception to the requirement to honor a do-not-call request. The TSR prohibits telemarketers and sellers from calling a consumer who has made a do-not-call request, unless the call falls under one of the specific exemptions, such as calls from or on behalf of tax-exempt nonprofit organizations, calls to consumers with whom the seller has an established business relationship, or calls to consumers who have given prior express written consent.
When the entity manages user preferences through multiple platforms. This is not an excuse for not sharing a do-not-call request across its organization. The TSR requires telemarketers and sellers to maintain an internal do-not-call list of consumers who have asked them not to call again, and to update the list at least once every 31 days. The entity must ensure that the do-not-call request is recorded and communicated across all of its platforms that are used for telemarketing purposes.

QUESTION 19
Within what time period must a commercial message sender remove a recipient's address once they have asked to stop receiving future e-mail?

A. 7 days
B. 10 days
C. 15 days
D. 21 days

Answer: B
Explanation:
According to the CAN-SPAM Act of 2003, a federal law that regulates commercial email messages, a commercial message sender must honor a recipient's opt-out request within 10 business days. The sender must provide a clear and conspicuous way for the recipient to opt out of receiving future emails, such as a link or an email address. The sender must not charge a fee, require the recipient to provide any personal information, or make the recipient take any steps other than sending a reply email or visiting a single web page to opt out. The sender must also not sell, exchange, or transfer the email address of the recipient who has opted out, unless it is necessary to comply with the law or prevent fraud.

QUESTION 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:
The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of students' educational records. FERPA generally requires schools to obtain written consent from students before disclosing their records to third parties, such as parents. However, FERPA allows some exceptions to this rule, such as when the disclosure is for health or safety emergencies, or when the student is still a dependent for tax purposes. According to FERPA, a school may disclose educational records to the parents of a student who is claimed as a dependent on the parents' most recent federal income tax return, without the student's consent. This exception applies regardless of the student's age or enrollment status at a postsecondary institution.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**