IAPP.CIPP-US.v2025-09-17.q217

Exam Code:	CIPP-US
Exam Name:	Certified Information Privacy Professional/United States (CIPP/US)
Certification Provider:	IAPP
Free Question Number:	217
Version:	v2025-09-17
# of views:	106
# of Questions views:	2170
https://www.exam-tests.com/CIPP-US-exam/IAPP.CIPP-US.v2025-09-17.q217.html	

NEW QUESTION: 1
Which act violates the Family Educational Rights and Privacy Act of 1974 (FERPA)?
A. A K-12 assessment vendor obtains a student's signed essay about her hometown from her school to use as an exemplar for public release
B. A university posts a public student directory that includes names, hometowns, e-mail addresses, and majors
C. A newspaper prints the names, grade levels, and hometowns of students who made the quarterly honor roll
D. University police provide an arrest report to a student's hometown police, who suspect him of a similar crime
Answer: A (LEAVE A REPLY)
The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of student education records. FERPA grants parents or eligible students the right to access, amend, and control the disclosure of their education records, with some exceptions. Schools must obtain written consent from the parent or eligible student before disclosing any personally identifiable information from the education records, unless an exception applies123 Option A violates FERPA because it involves the disclosure of a student's personally identifiable information (PII) from the education records without consent. A student's signed essay about her hometown is considered an education record under FERPA, as it is directly related to the student and maintained by the school12 A K-
12 assessment vendor is not a school official with a legitimate educational interest, nor does it fall under any of the exceptions that allow disclosure without consent12 Therefore, the school must obtain the student's (or the parent's, if the student is a minor) written consent before providing the essay to the vendor for public release.

Option B does not violate FERPA because it involves the disclosure of directory information, which is not considered PII under FERPA. Directory information is information that would not generally be considered harmful or an invasion of privacy if disclosed, such as name, address, phone number, e-mail address, major, etc12 Schools may disclose directory information without consent, unless the parent or eligible student has opted out of such disclosure12 However, schools must notify parents and eligible students of the types of directory information they designate and their right to opt out annually12 Option C does not violate FERPA because it involves the disclosure of information that is not part of the education records. FERPA only applies to education records that are directly related to a student and maintained by the school or a party acting for the school12 A newspaper's publication of the names, grade levels, and hometowns of students who made the quarterly honor roll is not based on the education records, but on the newspaper's own sources and reporting. Therefore, FERPA does not prohibit such disclosure.
Option D does not violate FERPA because it involves the disclosure of information under an exception that allows disclosure without consent. FERPA permits schools to disclose education records, or PII from education records, without consent to comply with a judicial order or lawfully issued subpoena, or to appropriate officials in connection with a health or safety emergency123 If the university police provide an arrest report to the student's hometown police in response to a subpoena or to prevent a serious threat to the student or others, they are not violating FERPA.
References: 1: Family Educational Rights and Privacy Act - Wikipedia 2: Family Educational Rights and Privacy Act (FERPA) | CDC 3: What is FERPA? | Protecting Student Privacy - ed

NEW QUESTION: 2
Due to cookie deprecation, businesses will be required to simplify their tracking practices by doing what?
A. Ensuring only registered users are tracked.
B. Running analytics only in dedicated sandboxes
C. Purging existing IDs that identify visitors by browser.
D. Deleting their existing data sets of any third-party cookies
Answer: (SHOW ANSWER)
With the impending deprecation of third-party cookies, businesses must simplify their tracking practices and shift to more privacy-conscious technologies. Third-party cookies are being phased out by major web browsers, such as Google Chrome, to improve user privacy and reduce cross- site tracking.
One of the most critical actions businesses need to take is deleting existing data sets of third- party cookies, as they will soon become obsolete. This action ensures compliance with emerging privacy standards and helps organizations transition to alternative methods of tracking, such as first-party data collection or consent-based tracking mechanisms.

NEW QUESTION: 3
Which of the following laws is NOT involved in the regulation of employee background checks?
A. The Civil Rights Act.
B. The Gramm-Leach-Bliley Act (GLBA).
C. The U.S. Fair Credit Reporting Act (FCRA).
D. The California Investigative Consumer Reporting Agencies Act (ICRAA).
Answer: B (LEAVE A REPLY)
The law that is not involved in the regulation of employee background checks is B. The Gramm- Leach-Bliley Act (GLBA). The GLBA is a federal law that regulates the privacy and security of financial information collected, used, or shared by financial institutions, such as banks, insurance companies, or securities firms. The GLBA does not apply to employee background checks, unless the employer is a financial institution that obtains financial information from a consumer reporting agency for employment purposes. In that case, the employer must comply with the GLBA's notice and opt-out requirements, as well as the FCRA's requirements for using consumer reports.

NEW QUESTION: 4
What is the most important action an organization can take to comply with the FTC position on retroactive changes to a privacy policy?
A. Describing the policy changes on its website.
B. Obtaining affirmative consent from its customers.
C. Publicizing the policy changes through social media.
D. Reassuring customers of the security of their information.
Answer: (SHOW ANSWER)
The FTC has stated that it is a deceptive practice to make retroactive changes to a privacy policy that affect how a company uses or shares previously collected personal information, unless the company obtains affirmative consent from the affected consumers. This means that the company must clearly and conspicuously disclose the changes and obtain the consumers' express agreement to them. Simply describing the policy changes on the website, publicizing them through social media, or reassuring customers of the security of their information are not sufficient to comply with the FTC's position.

NEW QUESTION: 5
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 (LEAVE A REPLY)

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 individual1. 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 standards2. References:
* Summary of the HIPAA Privacy Rule
* Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

NEW QUESTION: 6
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: (SHOW ANSWER)
Most state laws require that a person or business that conducts business in the state and owns or licenses personal information of residents of that state must notify those residents of any breach of the security of the system involving their personal information. This means that the entity does not have to be physically located in the state, have employees in the state, or be registered inthe state to be subject to the breach notification requirements, as long as it conducts business in the state and holds personal information of state residents. Conducting business in the state can be interpreted broadly to include any transaction or activity that involves the state or its residents, such as selling goods or services, collecting payments, or maintaining a website accessible by state residents. The other options (B, C, and D) are not commonly required by most state laws, although some states may have additional or specific requirements for certain types of entities, such as information brokers, health care providers, or financial institutions. References:

* Security Breach Notification Chart | Perkins Coie
* Security Breach Notification Laws - National Conference of State Legislatures
* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4: State Privacy Laws and Regulations, Section 4.2: State Security Breach Notification Laws.

NEW QUESTION: 7
When designing contact tracing apps in relation to COVID-19 or any other diagnosed virus, all of the following privacy measures should be considered EXCEPT?
A. Data retention.
B. Use limitations.
C. Opt-out choice.
D. User confidentiality.
Answer: (SHOW ANSWER)
Opt-out choice is not typically a privacy measure considered in the design of contact tracing apps. Contact tracing apps are designed to help identify and notify individuals who may have been exposed to a contagious virus, such as COVID-19, in order to slow the spread of the virus. User participation in contact tracing is typically voluntary, and individuals can choose whether or not to use the app. Therefore, an opt-out choice is not directly related to the design of the app itself. Instead, it's more about user consent and participation. The other options (data retention, use limitations, and user confidentiality) are important privacy considerations in the design and operation of such apps.

NEW QUESTION: 8
Based on current US employment privacy laws, which of the following should NOT be expected to happen while employed with a company?
A. Taking a polygraph test due to a theft at work.
B. Video monitoring only for workplace safety compliance.
C. GPS tracking while making deliveries for work.
D. A manager accessing your computer to get an needed file while you are on vacation.
Answer: A (LEAVE A REPLY)
Under the Employee Polygraph Protection Act of 1988 (EPPA), employers are not allowed to use lie detectors?on workers or candidates.

NEW QUESTION: 9
Which act violates the Family Educational Rights and Privacy Act of 1974 (FERPA)?
A. A K-12 assessment vendor obtains a student's signed essay about her hometown from her school to use as an exemplar for public release
B. A university posts a public student directory that includes names, hometowns, e-mail addresses, and majors
C. A newspaper prints the names, grade levels, and hometowns of students who made the quarterly honor roll

D. University police provide an arrest report to a student's hometown police, who suspect him of a similar crime

Answer: (SHOW ANSWER)

The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of student education records. FERPA grants parents or eligible students the right to access, amend, and control the disclosure of their education records, with some exceptions.

Schools must obtain written consent from the parent or eligible student before disclosing any personally identifiable information from the education records, unless an exception applies.

Option A violates FERPA because it involves the disclosure of a student's personally identifiable information (PII) from the education records without consent. A student's signed essay about her hometown is considered an education record under FERPA, as it is directly related to the student and maintained by the school. A K-12 assessment vendor is not a school official with a legitimate educational interest, nor does it fall under any of the exceptions that allow disclosure without consent. Therefore, the school must obtain the student's (or the parent's, if the student is a minor) written consent before providing the essay to the vendor for public release. Option B does not violate FERPA because it involves the disclosure of directory information, which is not considered PII under FERPA. Directory information is information that would not generally be considered harmful or an invasion of privacy if disclosed, such as name, address, phone number, e- mail address, major, etc. Schools may disclose directory information without consent, unless the parent or eligible student has opted out of such disclosure. However, schools must notify parents and eligible students of the types of directory information they designate and their right to opt out annually.

Option C does not violate FERPA because it involves the disclosure of information that is not part of the education records. FERPA only applies to education records that are directly related to a student and maintained by the school or a party acting for the school. A newspaper's publication of the names, grade levels, and hometowns of students who made the quarterly honor roll is not based on the education records, but on the newspaper's own sources and reporting. Therefore, FERPA does not prohibit such disclosure.

Option D does not violate FERPA because it involves the disclosure of information under an exception that allows disclosure without consent. FERPA permits schools to disclose education records, or PII from education records, without consent to comply with a judicial order or lawfully issued subpoena, or to appropriate officials in connection with a health or safety emergency. If the university police provide an arrest report to the student's hometown police in response to a subpoena or to prevent a serious threat to the student or others, they are not violating FERPA.

NEW QUESTION: 10

Even when dealing with an organization subject to the CCPA, California residents are NOT legally entitled to request that the organization do what?
A. Delete their personal information.
B. Correct their personal information.
C. Disclose their personal information to them.
D. Refrain from selling their personal information to third parties.
Answer: B (LEAVE A REPLY)
The CCPA grants California residents the right to request that a business delete, disclose, or stop selling their personal information, but it does not grant them the right to request that a business correct their personal information. However, the CPRA, which will amend and expand the CCPA in 2023, will grant California residents the right to request that a business correct inaccurate personal information. References: CCPA, CPRA, IAPP CIPP/US Study Guide (p. 62)

NEW QUESTION: 11
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 (LEAVE A REPLY)
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.
The other options are not sufficient to comply with HIPAA. Stating the privacy policy verbally (option A) does not provide the individual with a written or electronic copy of the NPP that they can keep for future reference. Posting the privacy notice in a prominent location (option B) does not ensure that the individual receives the NPP or has an opportunity to review it before receiving services. Directing patients to the correct area of the hospital website (option C) does not provide the individual with the NPP at the time of service delivery, unless the individual agrees to receive the NPP electronically and has access to the website at that time. References:
* Notice of Privacy Practices for Protected Health Information
* Model Notices of Privacy Practices

* Sample Notice: Availability of Notice of Privacy Practices
* Notice of Privacy Practices
* Notice of Privacy Practices (NPP) Distribution and Acknowledgement

NEW QUESTION: 12
SCENARIO
Please use the following to answer the next question:
You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in statea. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo.
CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.
A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals ?ones that exposed the PHI of public figures including celebrities and politicians.
During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.
A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.
Of the safeguards required by the HIPAA Security Rule, which of the following is NOT at issue due to HealthCo's actions?
A. Administrative Safeguards
B. Technical Safeguards
C. Physical Safeguards
D. Security Safeguards
Answer: D (LEAVE A REPLY)
The HIPAA Security Rule requires covered entities and their business associates to implement three types of safeguards to protect the confidentiality, integrity, and availability

of electronic protected health information (ePHI): administrative, physical, and technical. Security safeguards is not a separate category of safeguards, but rather a general term that encompasses all three types. Therefore, it is not a correct answer to the question.
Administrative safeguards are the policies and procedures that govern the conduct of the workforce and the security measures put in place to protect ePHI. They include risk analysis and management, training, contingency planning, incident response, and evaluation. Physical safeguards are the locks, doors, cameras, and other physical measures that prevent unauthorized access to ePHI. They include workstation and device security, locks and keys, and disposal of media.
Technical safeguards are the software and hardware tools that protect ePHI from unauthorized access, alteration, or destruction. They include access control, encryption, audit controls, integrity controls, and transmission security.
In the scenario, HealthCo's actions have potentially violated all three types of safeguards. For example:
HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures. This could be a breach of the administrative safeguard of risk analysis and management.
HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. This could be a breach of the technical safeguard of encryption.
HealthCo provides its investigative report of the breach and a copy of the PHI of the individuals affected to law enforcement. This could be a breach of the physical safeguard of disposal of media, if HealthCo did not ensure that the media was properly erased or destroyed after the transfer.

NEW QUESTION: 13
What is the main reason some supporters of the European approach to privacy are skeptical about self- regulation of privacy practices?
A. A large amount of money may have to be sent on improved technology and security
B. Industries may not be strict enough in the creation and enforcement of rules
C. A new business owner may not understand the regulations
D. Human rights may be disregarded for the sake of privacy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
What role does the U.S. Constitution play in the area of workplace privacy?
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 (LEAVE A REPLY)

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. References:

* 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

NEW QUESTION: 15
Under the EU-US Data Privacy Framework, what must participating organizations provide to individuals in regard to complaints and disputes?
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.
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 16
A software company wants to use web scraping to collect personal data from professional networking websites in order to train an artificial intelligence program to evaluate Job applications. The company has identified several actions for limiting their potential legal liability regarding affected data subjects and professional networking websites. Which of the following would be the least effective action for helping them do this?
A. Following the terms of use posted on professional networking websites that are scraped.
B. Adding a notice to the company website's terms of use disclosing the use of web scraping
C. Limiting the amount of the personally identifiable information they collect
D. Decertifying the scraped data before selling it to any third parties.
Answer: B (LEAVE A REPLY)
Web scraping to collect personal data can pose significant legal and ethical risks, particularly when it involves professional networking sites or other platforms where terms of service (ToS) explicitly prohibit such activity.

To limit liability, the software company must take proactive measures to comply with applicable laws (such as privacy laws) and contractual obligations (e.g., terms of use on the scraped websites).
Adding a notice to the company website's terms of use would be the least effective action, as it does not address the legal and ethical issues associated with scraping data from third-party websites. Simply adding a notice about the company's use of scraping does not mitigate liability for violating the ToS of professional networking websites or violating privacy rights under laws like the GDPR or CCPA.
Explanation of Options:
* A. Following the terms of use posted on professional networking websites that are scraped:This is one of the most effective ways to limit legal liability. Violating ToS can result in lawsuits or legal penalties, so adhering to them is critical.
* B. Adding a notice to the company website's terms of use disclosing the use of web scraping:This is the least effective action. Including this notice on the company's own website does not address potential violations of third-party website ToS or the privacy rights of affected individuals.
* C. Limiting the amount of the personally identifiable information they collect:Minimizing the amount of data collected aligns with data protection principles, such as data minimization under the GDPR, and can reduce privacy risks.
* D. Deidentifying the scraped data before selling it to any third parties:Deidentifying or anonymizing data is a critical step for reducing legal liability and complying with privacy laws.
However, the company should also ensure that the deidentification is robust and irreversible.
References from CIPP/US Materials:
* GDPR Article 5: Establishes principles such as data minimization and accountability for data processing.
* IAPP CIPP/US Certification Textbook: Highlights the risks of web scraping and the importance of adhering to contractual obligations and privacy laws.

NEW QUESTION: 17
Which federal act does NOT contain provisions for preempting stricter state laws?

A. The CAN-SPAM Act
B. The Children's Online Privacy Protection Act (COPPA)
C. The Telemarketing Consumer Protection and Fraud Prevention Act
D. The Fair and Accurate Credit Transactions Act (FACTA)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
What is the main purpose of the CAN-SPAM Act?
A. To diminish the use of electronic messages to send sexually explicit materials
B. To authorize the states to enforce federal privacy laws for electronic marketing
C. To empower the FTC to create rules for messages containing sexually explicit content
D. To ensure that organizations respect individual rights when using electronic advertising
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

NEW QUESTION: 19
Even when dealing with an organization subject to the CCPA, California residents are NOT legally entitled to request that the organization do what?
A. Delete their personal information.
B. Correct their personal information.
C. Disclose their personal information to them.
D. Refrain from selling their personal information to third parties.
Answer: B (LEAVE A REPLY)
The CCPA grants California residents the right to request that a business delete, disclose, or stop selling their personal information, but it does not grant them the right to request that a business correct their personal information. However, the CPRA, which will amend and expand the CCPA in 2023, will grant California residents the right to request that a business correct inaccurate personal information.

NEW QUESTION: 20
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?
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 (LEAVE A REPLY)
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.
References 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.

NEW QUESTION: 21
Which of the following best describes how federal anti-discrimination laws protect the privacy of private-sector employees in the United States?
A. They prescribe working environments that are safe and comfortable.
B. They limit the amount of time a potential employee can be interviewed.
C. They promote a workforce of employees with diverse skills and interests.
D. They limit the types of information that employers can collect about employees.
Answer: D (LEAVE A REPLY)

Federal anti-discrimination laws, such as Title VII of the Civil Rights Act of 1964, the Equal Pay Act of 1963, the Age Discrimination in Employment Act of 1967, and the Americans with Disabilities Act of 1990, prohibit employers from discriminating against employees or applicants based on certain protected characteristics, such as race, color, religion, sex, national origin, age, disability, and genetic information. These laws also limit the types of information that employers can collect, use, disclose, or retain about employees or applicants, in order to prevent discrimination or invasion of privacy. For example, employers cannot ask about an applicant's medical history, disability status, genetic information, or religious beliefs, unless they are relevant to the job or a bona fide occupational qualification. Employers also cannot use such information to make adverse employment decisions, such as hiring, firing, promotion, or compensation, unless they are justified by a legitimate business necessity or a reasonable accommodation.
Employers must also safeguard the confidentiality of such information and dispose of it properly when it is no longer needed.

NEW QUESTION: 22
Most states with data breach notification laws indicate that notice to affected individuals must be sent in the
"most expeditious time possible without unreasonable delay." By contrast, which of the following states currently imposes a definite limit for notification to affected individuals?
A. Maine
B. Florida
C. New York
D. California
Answer: (SHOW ANSWER)
According to the web search results from my predefined tool, Florida is the only state among the four options that currently imposes a definite limit for notification to affected individuals in case of a data breach. Florida's law requires that notice be provided within 30 days after determination of the breach or reason to believe a breach occurred, unless delayed by law enforcement or measures to determine the scope of the breach and restore the integrity of the system1. The other states have more flexible or vague terms for the notification timeframe, such as "as soon as practicable" (Maine), "in the most expedient time possible and without unreasonable delay" (New York), or "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement" (California)2. References:
* Security Breach Notification Chart | Perkins Coie
* State Data Breach Notification Chart - International Association of ...

NEW QUESTION: 23
Which of the following privacy rights is NOT available under the Colorado Privacy Act?
A. The right to access sensitive data.

B. The right to correct sensitive data.
C. The right to delete sensitive data.
D. The right to limit the use of sensitive data.
Answer: D (LEAVE A REPLY)
The Colorado Privacy Act (CPA) grants consumers the right to access, correct, or delete their personal data, including sensitive data, that is processed by a controller. Sensitive data is defined as personal data that reveals racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, genetic or biometric data, or personal data from a known child. The CPA also grants consumers the right to opt out of the processing of their personal data for purposes of targeted advertising, the sale of personal data, or certain kinds of profiling. However, the CPA does not grant consumers the right to limit the use of sensitive data for other purposes, such as providing a product or service requested by the consumer, complying with legal obligations, or protecting the vital interests of the consumer or another person. Therefore, option D is the correct answer, as it is not a privacy right available under the CPA.

NEW QUESTION: 24
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 (LEAVE A REPLY)
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.

NEW QUESTION: 25
The Family Educational Rights and Privacy Act (FERPA) requires schools to do all of the following EXCEPT?
A. Verify the identity of students who make requests for access to their records.
B. Provide students with access to their records within a specified amount of time.
C. Respond to all reasonable student requests regarding explanation of their records.
D. Obtain student authorization before releasing directory information in their records.
Answer: (SHOW ANSWER)
The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records and gives parents or eligible students the right to access, amend, and control the disclosure of their records. FERPA applies to all educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education12 FERPA requires schools to do all of the following:
* Verify the identity of students who make requests for access to their records. Schools must use reasonable methods to identify and authenticate the identity of parents, students, school officials, and any other parties to whom they disclose education records12
* Provide students with access to their records within a specified amount of time. Schools must provide parents or eligible students with an opportunity to inspect and review the student's education records within 45 days of receiving a request. Schoolsare not required to provide copies of records unless it is impossible for parents or eligible students to review the records at the school12
* Respond to all reasonable student requests regarding explanation of their records. Schools must provide parents or eligible students with an opportunity to request the amendment of the student's education records that they believe are inaccurate, misleading, or otherwise in violation of the student's privacy rights. Schools must consider the request and decide whether to amend the records within a reasonable time. If the school decides not to amend the records, it must inform the parent or eligible student of their right to a hearing on the matter12 FERPA does not require schools to do the following:

* Obtain student authorization before releasing directory information in their records. Directory information is information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed. Examples of directory information include the student's name, address, phone number, e-mail address, date and place of birth, major field of study, participation in sports and activities, dates of attendance, degrees and awards received, and most recent school attended. Schools may disclose directory information without consent unless the parent or eligible student has opted out of such disclosure. Schools must notify parents and eligible students of the types of information they designate as directory information and of their right to opt out of directory information disclosure12 Therefore, the correct answer is D. Obtain student authorization before releasing directory information in their records.
References:
* Family Educational Rights and Privacy Act (FERPA)
* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4: Federal Privacy Laws, Section 4.3: The Family Educational Rights and Privacy Act (FERPA)

NEW QUESTION: 26
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 (LEAVE A REPLY)
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. References:
* Vendor Selection Process: a Step-by-Step Guide, section "Step 2: Define the vendor selection criteria"
* [IAPP CIPP/US Study Guide], p. 81-82, section 3.4.1
* [IAPP CIPP/US Body of Knowledge], p. 18-19, section C.2.a

NEW QUESTION: 27
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.
Under the General Data Protection Regulation (GDPR), how would the U.S.-based startup company most likely be classified?
A. As a data supervisor
B. As a data processor
C. As a data controller
D. As a data manager
Answer: (SHOW ANSWER)
The data privacy leader needs to identify all the personal data that the Company has received from the retailer, as well as the purposes, retention periods, and sharing practices of such data.
Since the data inventory is obsolete, the data privacy leader cannot rely on it to provide accurate and complete information. Therefore, the next best source of information is to interview the key marketing personnel who are responsible for the partnership with the retailer and the use of the personal data. The marketing personnel can provide insights into the data flows, the data categories, the data processing activities, and the data protection measures that the Company has implemented. They can also help the data privacy leader to locate the relevant documents, contracts, and records that can support the investigation.

NEW QUESTION: 28
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 homework?" 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
QUESTION s 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.
Depending on where Matt lives, the marketer could be prosecuted for violating which of the following?
A. Red Flag Rules.
B. Investigative Consumer Reporting Agencies Act.
C. Unfair and Deceptive Acts and Practices laws.
D. Consumer Bill of Rights.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
SCENARIO
Please use the following to answer the next QUESTION:
Cheryl is the sole owner of Fitness Coach, Inc., a medium-sized company that helps individuals realize their physical fitness goals through classes, individual instruction, and access to an extensive indoor gym. She has owned the company for ten years and has always been concerned about protecting customer's privacy while maintaining the highest level of service. She is proud that she has built long-lasting customer relationships.
Although Cheryl and her staff have tried to make privacy protection a priority, the company has no formal privacy policy. So Cheryl hired Janice, a privacy professional, to help her develop one.

After an initial assessment, Janice created a first of a new policy. Cheryl read through the draft and was concerned about the many changes the policy would bring throughout the company. For example, the draft policy stipulates that a customer's personal information can only be held for one year after paying for a service such as a session with personal trainer. It also promises that customer information will not be shared with third parties without the written consent of the customer. The wording of these rules worry Cheryl since stored personal information often helps her company to serve her customers, even if there are long pauses between their visits. In addition, there are some third parties that provide crucial services, such as aerobics instructors who teach classes on a contract basis. Having access to customer files and understanding the fitness levels of their students helps instructors to organize their classes.

Janice understood Cheryl's concerns and was already formulating some ideas for revision. She tried to put Cheryl at ease by pointing out that customer data can still be kept, but that it should be classified according to levels of sensitivity. However, Cheryl was skeptical. It seemed that classifying data and treating each type differently would cause undue difficulties in the company's day-to-day operations. Cheryl wants one simple data storage and access system that any employee can access if needed.

Even though the privacy policy was only a draft, she was beginning to see that changes within her company were going to be necessary. She told Janice that she would be more comfortable with implementing the new policy gradually over a period of several months, one department at a time. She was also interested in a layered approach by creating documents listing applicable parts of the new policy for each department.

Based on the scenario, which of the following would have helped Janice to better meet the company's needs?

A. Creating a more comprehensive plan for implementing a new policy

B. Spending more time understanding the company's information goals

C. Explaining the importance of transparency in implementing a new policy

D. Removing the financial burden of the company's employee training program

Answer: B (LEAVE A REPLY)

According to the Wiley study guide, one of the steps in developing a privacy policy is to conduct a privacy assessment, which involves identifying the organization's information goals and needs, as well as the legal and regulatory requirements that apply to its data collection and use practices3. By spending more time understanding the company's information goals, Janice would have been able to tailor the privacy policy to fit the company's business model and customer expectations, while still complying with the relevant privacy laws and standards. This would have also helped Janice to address Cheryl's concerns about the impact of the policy on the company's operations and customer relationships, and to propose solutions that balance privacy protection and service delivery.

References:

1: https://iapp.org/certify/cippus/

2: https://iapp.org/certify/get-certified/cippus/
3: https://www.wiley.com/en-be
/IAPP+CIPP+US+Certified+Information+Privacy+Professional+Study+Guide-
p-9781119755517
4: https://www.techtarget.com/searchsecurity/quiz/10-CIPP-US-practice-questions-to-test-
your-privacy- knowledge
5: https://www.study4exam.com/iapp/free-cipp-us-questions
https://www.passitcertify.com/iapp/cipp-us-questions.html

NEW QUESTION: 30
What consumer service was the Fair Credit Reporting Act (FCRA) originally intended to provide?
A. The ability to receive reports from multiple credit reporting agencies.
B. The ability to appeal negative credit-based decisions.
C. The ability to correct inaccurate credit information.
D. The ability to investigate incidents of identity theft.
Answer: C (LEAVE A REPLY)
, "..Specifically, FCRA mandates accurate and relevant data collection, provides consumers with the ability to access and correct their information, and limits the use of consumer reports to defined permissible purposes".

NEW QUESTION: 31
Which of the following became the first state to pass a law specifically regulating the collection of biometric data?
A. California.
B. Texas.
C. Illinois.
D. Washington.
Answer: C (LEAVE A REPLY)
Illinois became the first state to pass a law specifically regulating the collection of biometric data in 2008, when it enacted the Biometric Information Privacy Act (BIPA). BIPA defines biometric identifiers as retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry, and biometric information as any information based on biometric identifiers used to identify an individual. BIPA requires entities that collect, store, or use biometric identifiers or information to obtain informed consent from individuals, provide written policies on data retention and destruction, limit disclosure and sale of biometric data, and protect biometric data using reasonable security measures. BIPA also provides a private right of action for individuals whose biometric data is collected, stored, or used in violation of the law, and allows them to recover statutory damages of $1,000 or actual damages, whichever is greater, for each negligent violation, and $5,000 or actual damages,

whichever is greater, for each intentional or reckless violation, as well as attorneys' fees and costs, and injunctive relief.

NEW QUESTION: 32
The rules for "e-discovery" mainly prevent which of the following?
A. A conflict between business practice and technological safeguards
B. The loss of information due to poor data retention practices
C. The practice of employees using personal devices for work
D. A breach of an organization's data retention program
Answer: B (LEAVE A REPLY)
Page 346 of the learning material - ".....e-discovery rules, which require automated and large-scale production of emails and other corporate documents during the discovery process prior to trial".

NEW QUESTION: 33
SCENARIO
Please use the following to answer the next question:
Noah is trying to get a new job involving the management of money. He has a poor personal credit rating, but he has made better financial decisions in the past two years. One potential employer, Arnie's Emporium, recently called to tell Noah he did not get a position.
As part of the application process, Noah signed a consent form allowing the employer to request his credit report from a consumer reporting agency (CRA). Noah thinks that the report hurt his chances, but believes that he may not ever know whether it was his credit that cost him the job.
However, Noah is somewhat relieved that he was not offered this particular position. He noticed that the store where he interviewed was extremely disorganized. He imagines that his credit report could still be sitting in the office, unsecured.
Two days ago, Noah got another interview for a position at Sam's Market. The interviewer told Noah that his credit report would be a factor in the hiring decision. Noah was surprised because he had not seen anything on paper about this when he applied.

Regardless, the effect of Noah's credit on his employability troubles him, especially since he has tried so hard to improve it. Noah made his worst financial decisions fifteen years ago, and they led to bankruptcy. These were decisions he made as a young man, and most of his debt at the time consisted of student loans, credit card debt, and a few unpaid bills ?all of which Noah is still working to pay off. He often laments that decisions he made fifteen years ago are still affecting him today.
In addition, Noah feels that an experience investing with a large bank may have contributed to his financial troubles. In 2007, in an effort to earn money to help pay off his debt, Noah talked to a customer service representative at a large investment company who urged him to purchase stocks. Without understanding the risks, Noah agreed. Unfortunately, Noah lost a great deal of money.
After losing the money, Noah was a customer of another financial institution that suffered a large security breach. Noah was one of millions of customers whose personal information was compromised. He wonders if he may have been a victim of identity theft and whether this may have negatively affected his credit.
Noah hopes that he will soon be able to put these challenges behind him, build excellent credit, and find the perfect job.
Consumers today are most likely protected from situations like the one Noah had buying stock because of which federal action or legislation?
A. The rules under the Fair Debt Collection Practices Act.
B. The creation of the Consumer Financial Protection Bureau.
C. Federal Trade Commission investigations into "unfair and deceptive" acts or practices.
D. Investigations of "abusive" acts and practices under the Dodd-Frank Wall Street Reform and Consumer Protection Act.
Answer: (SHOW ANSWER)
The Dodd-Frank Act was established to prevent the risky financial practices that led to the 2007?008 financial crisis, which included issues similar to Noah's experience with buying stocks without understanding the risks. The act includes provisions for consumer protection in financial services and aims to prevent abusive practices in the financial industry.

NEW QUESTION: 34
Which act violates the Family Educational Rights and Privacy Act of 1974 (FERPA)?
A. A K-12 assessment vendor obtains a student's signed essay about her hometown from her school to use as an exemplar for public release
B. A university posts a public student directory that includes names, hometowns, e-mail addresses, and majors
C. A newspaper prints the names, grade levels, and hometowns of students who made the quarterly honor roll
D. University police provide an arrest report to a student's hometown police, who suspect him of a similar crime

Answer: (SHOW ANSWER)

The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of student education records. FERPA grants parents or eligible students the right to access, amend, and control the disclosure of their education records, with some exceptions. Schools must obtain written consent from the parent or eligible student before disclosing any personally identifiable information from the education records, unless an exception applies123 Option A violates FERPA because it involves the disclosure of a student's personally identifiable information (PII) from the education records without consent. A student's signed essay about her hometown is considered an education record under FERPA, as it is directly related to the student and maintained by the school12 A K-12 assessment vendor is not a school official with a legitimate educational interest, nor does it fall under any of the exceptions that allow disclosure without consent12 Therefore, the school must obtain the student's (or the parent's, if the student is a minor) written consent before providing the essay to the vendor for public release.

Option B does not violate FERPA because it involves the disclosure of directory information, which is not considered PII under FERPA. Directory information is information that would not generally be considered harmful or an invasion of privacy if disclosed, such as name, address, phone number, e-mail address, major, etc12 Schools may disclose directory information without consent, unless the parent or eligible student has opted out of such disclosure12 However, schools must notify parents and eligible students of the types of directory information they designate and their right to opt out annually12 Option C does not violate FERPA because it involves the disclosure of information that is not part of the education records. FERPA only applies to education records that are directly related to a student and maintained by theschool or a party acting for the school12 A newspaper's publication of the names, grade levels, and hometowns of students who made the quarterly honor roll is not based on the education records, but on the newspaper's own sources and reporting. Therefore, FERPA does not prohibit such disclosure.

Option D does not violate FERPA because it involves the disclosure of information under an exception that allows disclosure without consent. FERPA permits schools to disclose education records, or PII from education records, without consent to comply with a judicial order or lawfully issued subpoena, or to appropriate officials in connection with a health or safety emergency123 If the university police provide an arrest report to the student's hometown police in response to a subpoena or to prevent a serious threat to the student or others, they are not violating FERPA.

References: 1: Family Educational Rights and Privacy Act - Wikipedia 2: Family Educational Rights and Privacy Act (FERPA) | CDC 3: What is FERPA? | Protecting Student Privacy - ed

NEW QUESTION: 35

SCENARIO

Please use the following to answer the next QUESTION:

Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. "If they were really serious about not being bothered," Evan said, "They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to." Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call "another time." This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.

Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social medi a. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions. Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.

Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.

Larry wants to take action, but is uncertain how to proceed.

Which act would authorize Evan's undercover investigation?

A. The National Labor Relations Act (NLRA)

B. The Whistleblower Protection Act

C. The Fair and Accurate Credit Transactions Act (FACTA)

D. The Stored Communications Act (SCA)

Answer: A (LEAVE A REPLY)

NEW QUESTION: 36

According to the FTC Report of 2012, what is the main goal of Privacy by Design?

A. Obtaining consumer consent when collecting sensitive data for certain purposes

B. Incorporating privacy protections throughout the development process

C. Implementing a system of standardization for privacy notices

D. Establishing a system of self-regulatory codes for mobile-related services
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Who is responsible for notifying consumers when adverse action is taken based on information in a consumer credit report?
A. The Credit Bureau
B. The User
C. The Credit Reporting Agency
D. The Consumer Financial Protection Bureau
Answer: B (LEAVE A REPLY)
Under the FCRA users must notify consumers when third-party (CRA) data is used to make adverse decisions about them.

NEW QUESTION: 38
In most cases, the FTC settles disputes through consent decrees and consent orders. What is the maximum length of a consent decree?
A. 5 years
B. 10 years
C. 20 years
D. Indefinitely
Answer: C (LEAVE A REPLY)
A consent decree can be imposed for up to 20 years.

NEW QUESTION: 39
According to FERPA, when can a school disclose records without a student's consent?
A. If the disclosure is not to be conducted through email to the third party
B. If the disclosure would not reveal a student's student identification number
C. If the disclosure is to practitioners who are involved in a student's health care
D. If the disclosure is to provide transcripts to a school where a student intends to enroll
Answer: (SHOW ANSWER)
According to FERPA, a school may disclose personally identifiable information (PII) from an eligible student's education records without consent if the disclosure meets one of the exceptions in 34 CFR ?99.. One of these exceptions is for disclosures to other schools to which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer (34 CFR ?99.31(a)(2)). This exception allows schools to disclose transcripts, recommendations, or other information that may facilitate the student's admission or enrollment at another school. However, the school must make a reasonable attempt to notify the student of the disclosure, unless the student initiated the disclosure, and must provide the student with a copy of the records that were disclosed upon request (34 CFR ?99.34(a)(1)).

NEW QUESTION: 40
SCENARIO
Please use the following to answer the next QUESTION:
You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data.
However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.
A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals - ones that exposed the PHI of public figures including celebrities and politicians.
During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.
A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.
What is the most effective kind of training CloudHealth could have given its employees to help prevent this type of data breach?
A. Training on techniques for identifying phishing attempts
B. Training on the terms of the contractual agreement with HealthCo
C. Training on the difference between confidential and non-public information
D. Training on CloudHealth's HR policy regarding the role of employees involved data breaches
Answer: A (LEAVE A REPLY)
Phishing is a form of social engineering that involves sending fraudulent emails or other messages that appear to come from a legitimate source, but are designed to trick recipients into revealing sensitive information, such as passwords, account numbers, or personal identifiers1. Phishing is one of the most common and effective methods of

cyberattacks, and it can lead to data breaches, identity theft, ransomware infections, or other serious consequences2. Therefore, training on how to recognize and avoid phishing attempts is crucial for any organization that handles sensitive data, especially ePHI, which is subject to strict regulations under HIPAA3. Training on techniques for identifying phishing attempts can help employees to spot the signs of a phishing email, such as:
* Sender's address or domain name that does not match the expected source or contains spelling errors4
* Generic salutations or impersonal tone that do not address the recipient by name or use proper grammar4
* Urgent or threatening language that creates a sense of pressure or fear and asks the recipient to take immediate action, such as clicking on a link, opening an attachment, or providing information4
* Suspicious links or attachments that may contain malware or lead to fake websites that mimic the appearance of a legitimate site, but have a different URL or request login credentials or other data4
* Requests for sensitive information that are unusual or out of context, such as asking for passwords, account numbers, or personal identifiers that the sender should already have or should not need4 Training on techniques for identifying phishing attempts can also help employees to learn how to respond to a phishing email, such as:
* Not clicking on any links or opening any attachments in the email4
* Not replying to the email or providing any information to the sender4
* Reporting the email to the IT department or security team and deleting it from the inbox4
* Verifying the legitimacy of the email by contacting the sender directly using a different channel, such as phone or another email address4
* Updating the antivirus software and scanning the device for any malware infection4
Training on techniques for identifying phishing attempts is the most effective kind of training that CloudHealth could have given its employees to help prevent this type of data breach, because it would have enabled them to recognize the phishing email that compromised the PHI of more than 10,000 HealthCo patients, and to avoid falling victim to it. Training on the terms of the contractual agreement with HealthCo, the difference between confidential and non-public information, or CloudHealth's HR policy regarding the role of employees involved in data breaches, while important, would not have been as effective in preventing this specific type of data breach, because they would not have addressed the root cause of the breach, which was the phishing email.
References:
* 1: IAPP, Phishing, https://iapp.org/resources/glossary/phishing/
* 2: SpinOne, The Top 5 Phishing Awareness Training Providers 2023, https://spinbackup.com/blog
/phishing-awareness-training-best-providers/
* 3: IAPP, HIPAA, https://iapp.org/resources/glossary/hipaa/
* 4: Expert Insights, The Top 11 Phishing Awareness Training and Simulation Solutions,

https://expertinsights.com/insights/the-top-11-phishing-awareness-training-and-simulation-solutions/

NEW QUESTION: 41
The use of cookies on a website by a service provider is generally not deemed a 'sale' of personal information by CCPA, as long as which of the following conditions is met?
A. The third party stores personal information to trigger a response to a consumer's request to exercise their right to opt in.
B. The analytics cookies placed by the service provider are capable of being tracked but cannot be linked to a particular consumer of that business.
C. The service provider retains personal information obtained in the course of providing the services specified in the agreement with the subcontractors.
D. The information collected by the service provider is necessary to perform debugging and the business and service provider have entered into an appropriate agreement.
Answer: D (LEAVE A REPLY)
The California Consumer Privacy Act (CCPA) defines a 'sale' of personal information as any transfer or disclosure of personal information to another business or third party for monetary or other valuable consideration. However, the CCPA also provides some exceptions to this definition, such as:
* If the consumer has directed the business to intentionally disclose the personal information or use the personal information to interact with a third party, provided the third party does not also sell the personal information.
* If the business transfers the personal information to a service provider that is contractually prohibited from retaining, using, or disclosing the personal information for any purpose other than performing the services specified in the contract with the business.
* If the business transfers the personal information to a third party as part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided the information is used or shared consistently with the CCPA.
The use of cookies on a website by a service provider is generally not deemed a sale of personal information by the CCPA, as long as the information collected by the service provider is necessary to perform the services specified in the contract with the business,and the service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose. One of the examples of a valid business purpose is to perform debugging to identify and repair errors that impair existing intended functionality.
Therefore, option D is the correct answer, as it describes a scenario where the use of cookies by a service provider is not a sale of personal information under the CCPA, assuming the service provider complies with the contractual obligations and does not further use or disclose the information.

Option A is incorrect, as it does not describe a valid exception to the definition of a sale. The third party that stores personal information to trigger a response to a consumer's request to opt in is not acting as a service provider, but as a separate entity that may have its own interest in the personal information. The consumer's request to opt in does not necessarily imply that the consumer has directed the business to disclose the personal information to the third party.
Option B is incorrect, as it does not describe a valid exception to the definition of a sale. The analytics cookies placed by the service provider may still constitute a sale of personal information, even if they cannot be linked to a particular consumer of that business. The CCPA defines personal information broadly to include any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Therefore, the analytics cookies may still fall within the scope of personal information, and their use by the service provider may still be a sale, unless one of the exceptions applies.
Option C is incorrect, as it does not describe a valid exception to the definition of a sale. The service provider that retains personal information obtained in the course of providing the services specified in the agreement with the subcontractors is not acting as a service provider to the business, but as a separate entity that may have its own interest in the personal information. The agreement with the subcontractors does not necessarily imply that the business has authorized the service provider to retain, use, or disclose the personal information for any purpose other than performing the services specified in the contract with the business.
References:
* [IAPP CIPP/US Study Guide], Chapter 10: California Consumer Privacy Act, pp. 223-226.
* CIPP/US Practice Questions (Sample Questions), Question 30.

NEW QUESTION: 42
When does the Telemarketing Sales Rule require an entity to share a do-not-call request across its organization?
A. When the goods and services sold by its divisions are very similar
B. When a call is not the result of an error or other unforeseen cause
C. When the operational structures of its divisions are not transparent
D. When the entity manages user preferences through multiple platforms
Answer: (SHOW ANSWER)

NEW QUESTION: 43
According to FERPA, when can a school disclose records without a student's consent?
A. If the disclosure is not to be conducted through email to the third party
B. If the disclosure would not reveal a student's student identification number
C. If the disclosure is to practitioners who are involved in a student's health care
D. If the disclosure is to provide transcripts to a school where a student intends to enroll

Answer: D (LEAVE A REPLY)
According to FERPA, a school may disclose personally identifiable information (PII) from an eligible student's education records without consent if the disclosure meets one of the exceptions in 34 CFR § 99.31.
One of these exceptions is for disclosures to other schools to which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer (34 CFR §
99.31(a)(2)). This exception allows schools to disclose transcripts, recommendations, or other information that may facilitate the student's admission or enrollment at another school. However, the school must make a reasonable attempt to notify the student of the disclosure, unless the student initiated the disclosure, and must provide the student with a copy of the records that were disclosed upon request (34 CFR § 99.34(a) (1)). References:
https://studentprivacy.ed.gov/ferpa
https://studentprivacy.ed.gov/ferpa

NEW QUESTION: 44
Which of the following best describes an employer's privacy-related responsibilities to an employee who has left the workplace?
A. An employer has a responsibility to permanently delete or expunge all sensitive employment records to minimize privacy risks to both the employer and former employee.
B. An employer has a responsibility to maintain a former employee's access to computer systems and company data needed to support claims against the company such as discrimination.
C. An employer may consider any privacy-related responsibilities terminated, as the relationship between employer and employee is considered primarily contractual.
D. An employer has a responsibility to maintain the security and privacy of any sensitive employment records retained for a legitimate business purpose.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
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: (SHOW ANSWER)
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.
The other options are not sufficient to comply with HIPAA. Stating the privacy policy verbally (option A) does not provide the individual with a written or electronic copy of the NPP that they can keep for future reference. Posting the privacy notice in a prominent location (option B) does not ensure that the individual receives the NPP or has an opportunity to review it before receiving services. Directing patients to the correct area of the hospital website (option C) does not provide the individual with the NPP at the time of service delivery, unless the individual agrees to receive the NPP electronically and has access to the website at that time. References:
* Notice of Privacy Practices for Protected Health Information
* Model Notices of Privacy Practices
* Sample Notice: Availability of Notice of Privacy Practices
* Notice of Privacy Practices
* Notice of Privacy Practices (NPP) Distribution and Acknowledgement

NEW QUESTION: 46
Don understands that some location-based services simply enhance the user experience. Others, such as daily fantasy sports applications that allow sports betting, require that location-based services be activated to function at all. Given Don's concern over his children's safety, which of the following best practices would you recommend to Don?
A. Do not allow the children to use location-based services at all.
B. Allow the children to turn on location-based services on their smart phones, but not their gaming consoles.
C. Allow the children to turn on location-based services on their gaming consoles, but not their smart phones.
D. Allow the children to turn on location-based services on all their devices.
Answer: (SHOW ANSWER)
Location-based services often just need to know the general area someone is in such as the state they are in now, and not their specific address. However, most mobile devices, like smart phones, are only used by a single individual. This complicates things because when that individual carries their mobile device everywhere with the location-based services turn on the identity of the person can be inferred based on their location, such as Sarah going to her middle school each day.
Since she is the only person in the family that attends the school each day, one could infer that she owns the device. Don should not allow location-based services on the smart

phone, or only allow location-based services to be activated when the children are home from school, or on the weekends.

NEW QUESTION: 47
Which statement is FALSE regarding the provisions of the Employee Polygraph Protection Act of 1988 (EPPA)?
A. The EPPA requires that employers post essential information about the Act in a conspicuous location.
B. The EPPA includes an exception that allows polygraph tests in professions in which employee honesty is necessary for public safety.
C. Employers are prohibited from administering psychological testing based on personality traits such as honesty, preferences or habits.
D. Employers involved in the manufacture of controlled substances may terminate employees based on polygraph results if other evidence exists.
Answer: (SHOW ANSWER)
Section: (none)
Explanation

NEW QUESTION: 48
What privacy concept grants a consumer the right to view and correct errors on his or her credit report?
A. Access.
B. Notice.
C. Action.
D. Choice.
Answer: (SHOW ANSWER)
Access is the privacy concept that grants a consumer the right to view and correct errors on his or her credit report. The Fair Credit Reporting Act (FCRA) gives consumers the right to access their credit reports from the three nationwide credit reporting agencies (Equifax, Experian, and TransUnion) once every 12 months for free. Consumers also have the right to dispute any inaccurate or incomplete information in their credit reports and request that the credit reporting agencies investigate and correct the errors. The FCRA also requires

the credit reporting agencies to provide consumers with a notice of their rights and a summary of the dispute process.

NEW QUESTION: 49
All of the following common law torts are relevant to employee privacy under US law EXCEPT?
A. Defamation
B. Intrusion upon seclusion.
C. Infliction of emotional distress.
D. Conversion.
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which of the following accurately describes the purpose of a particular federal enforcement agency?
A. The National Institute of Standards and Technology (NIST) has established mandatory privacy standards that can then be enforced against all for-profit organizations by the Department of Justice (DOJ).
B. The Cybersecurity and Infrastructure Security Agency (CISA) is authorized to bring civil enforcement actions against organizations whose website or other online service fails to adequately secure personal information.
C. The Federal Communications Commission (FCC) regulates privacy practices on the internet and enforces violations relating to websites' posted privacy disclosures.
D. The Federal Trade Commission (FTC) is typically recognized as having the broadest authority under the FTC Act to address unfair or deceptive privacy practices.
Answer: D (LEAVE A REPLY)
The FTC is the primary federal agency responsible for enforcing privacy and data security laws in the United States. The FTC has broad jurisdiction over most commercial entities that collect, use, or share personal information from consumers. The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce, which includes unfair or deceptive privacy practices. The FTC can bring enforcement actions against companies that violate their own privacy policies, fail to provide adequate notice or choice to consumers, engage in unfair or harmful data practices, or breach consumers' reasonable expectations of privacy. The FTC can also issue rules, guidelines, and reports on privacy and data security issues, as well as conduct investigations, workshops, and educational campaigns.

NEW QUESTION: 51
Acme Student Loan Company has developed an artificial intelligence algorithm that determines whether an individual is likely to pay their bill or default. A person who is determined by the algorithm to be more likely to default will receive frequent payment

reminder calls, while those who are less likely to default will not receive payment reminders.
Which of the following most accurately reflects the privacy concerns with Acme Student Loan Company using artificial intelligence in this manner?
A. If the algorithm uses risk factors that impact the automatic decision engine. Acme must ensure that the algorithm does not have a disparate impact on protected classes in the output.
B. If the algorithm makes automated decisions based on risk factors and public information, Acme need not determine if the algorithm has a disparate impact on protected classes.
C. If the algorithm's methodology is disclosed to consumers, then it is acceptable for Acme to have a disparate impact on protected classes.
D. If the algorithm uses information about protected classes to make automated decisions, Acme must ensure that the algorithm does not have a disparate impact on protected classes in the output.
Answer: (SHOW ANSWER)
https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms See above. Even the examples provided therein use public information, but result in disparate impacts, and therefore are subject to challenge by the FTC.

NEW QUESTION: 52
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: (SHOW ANSWER)
The scenario describes how the company had no adequate rules about access to customer information and how low-level employees had access to all of the company's customer data, including financial records. This indicates that the company did not implement proper access controls to limit who can access, use, or disclose customer information based on their roles and responsibilities. Access controls are one of the key elements of information security and privacy, as they help prevent unauthorized or inappropriate access to sensitive data.
Without access controls, the company's customer information was vulnerable to mishandling by employees or outsiders who could exploit the weaksecurity measures. Therefore, the most likely cause of the breach was mishandling of information caused by lack of access controls. References:
* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4: Information Management from a U.S. Perspective, Section 4.2: Information Security, p. 113-114
* IAPP CIPP/US Body of Knowledge, Domain I: Introduction to the U.S. Privacy Environment, Objective
I.C: Describe the role of information security in privacy, Subobjective I.C.1: Identify the key elements of information security, p. 8

NEW QUESTION: 53
Federal laws establish which of the following requirements for collecting personal information of minors under the age of 13?
A. Implied consent from a minor's parent or guardian, or affirmative consent from the minor.

B. Affirmative consent from a minor's parent or guardian before collecting the minor's personal information online.
C. Implied consent from a minor's parent or guardian before collecting a minor'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 (LEAVE A REPLY)
Explanation/Reference: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked- questions-0

NEW QUESTION: 54
Sarah lives in San Francisco, California. Based on a dramatic increase in unsolicited commercial emails, Sarah believes that a major social media platform with over 50 million users has collected a lot of personal information about her. The company that runs the platform is based in New York and France.
Why is Sarah entitled to ask the social media platform to delete the personal information they have collected about her?
A. Any company with a presence in Europe must comply with the General Data Protection Regulation globally, including in response to data subject deletion requests.
B. Under Section 5 of the FTC Act, the Federal Trade Commission has held that refusing to delete an individual's personal information upon request constitutes an unfair practice.
C. The California Consumer Privacy Act entitles Sarah to request deletion of her personal information.
D. The New York "Stop Hacks and Improve Electronic Data Security" (SHIELD) Act requires that businesses under New York's jurisdiction must delete customers' personal information upon request.
Answer: C (LEAVE A REPLY)
The correct answer is C because the California Consumer Privacy Act (CCPA) is a state privacy law that grants California residents the right to request the deletion of their personal information that a business has collected from them. The CCPA applies to any business that collects personal information from California residents, regardless of where the business is located, as long as the business meets certain thresholds of revenue, data volume, or data sharing. Therefore, the social media platform that Sarah uses is subject to the CCPA and must honor Sarah's deletion request, unless an exception applies. The CCPA also requires businesses to provide notice and choice to consumersabout their data collection and use practices, and to respond to consumer requests within 45 days.
The other answers are incorrect because:
* A is incorrect because the General Data Protection Regulation (GDPR) is a European Union privacy law that applies to the processing of personal data of individuals who are in the EU, regardless of where the data controller or processor is located. However, the GDPR does not apply to the processing of personal data of individuals who are outside the

EU, unless the processing relates to the offering of goods or services to such individuals or the monitoring of their behavior within the EU. Therefore, the GDPR does not apply to Sarah's personal data, since she is not in the EU and the social media platform is not targeting or tracking her in the EU.
* B is incorrect because Section 5 of the FTC Act is a federal law that prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC has used its Section 5 authority to enforce privacy and data security standards against businesses that violate their own privacy policies, misrepresent their data practices, or fail to protect consumer data from unauthorized access or disclosure. However, the FTC has not held that refusing to delete an individual's personal information upon request constitutes an unfair practice per se, unless the refusal is inconsistent with the business's privacy policy or representations, or causes substantial injury to consumers that is not reasonably avoidable or outweighed by countervailing benefits.
* D is incorrect because the New York SHIELD Act is a state law that imposes data breach notification and data security requirements on any person or business that owns or licenses computerized data that includes the private information of a New York resident. The SHIELD Act does not grant New York residents the right to request the deletion of their personal information, nor does it apply to businesses that do not collect or hold the private information of New York residents. Therefore, the SHIELD Act does not apply to Sarah's personal data, since she is not a New York resident and the social media platform may not have her private information as defined by the SHIELD Act. References:
* U.S. Private-Sector Privacy, Third Edition by Peter P. Swire, DeBrae Kennedy-Mayo, Chapter 7, Section 7.2.1, pp. 183-186.
* IAPP CIPP/US Certified Information Privacy Professional Study Guide by Mike Chapple and Joe Shelley, Chapter 7, Section 7.2, pp. 217-219.

NEW QUESTION: 55
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: (SHOW ANSWER)
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. Some of these objectives and measures include:
* Protect electronic protected health information (ePHI)
* Generate prescriptions electronically
* Implement clinical decision support (CDS)
* Use computerized provider order entry (CPOE) for medication, laboratory, and diagnostic imaging orders
* Timely patient access to electronic files
* Exchange health information with other providers and public health agencies
* Report clinical quality measures and public health data
Therefore, the correct answer is A. Making EHRs part of regular care is an important action that a health care provider must take if she wants to qualify for funds under the HITECH Act. References:
* What is the HITECH Act? 2024 Update, section "The Meaningful Use Program"
* The HITECH Act explained: Definition, compliance, and violations, section "HITECH Act definition and summary" and "Why was the HITECH Act created and why is it important?"
* Proposed Rulemaking to Implement HITECH Act Modifications, section "The Health Information Technology for Economic and Clinical Health (HITECH) Act"
* Health Information Technology for Economic and Clinical Health (HITECH) Audits, section "The American Recovery & Reinvestment Act of 2009 (ARRA, or Recovery Act)"
* What is HITECH Compliance? Understanding and Meeting HITECH Requirements, section "HITECH Compliance Requirements"

NEW QUESTION: 56
Which of the following entities is the PRIMARY enforcer of the HIPAA Privacy Rule and can assess civil monetary penalties?
A. Federal Trade Commission
B. Office of Civil Rights
C. State Attorney General
D. US Department of Justice
Answer: B (LEAVE A REPLY)
The Office of Civil Rights (OCR) is the primary enforcer of the HIPAA Privacy Rule. The U.S.
Department of Justice (DOJ) has criminal enforcement authority. The FTC and state attorneys general can bring enforcement for unfair and deceptive practices.

NEW QUESTION: 57
More than half of U.S. states require telemarketers to?
A. Identify themselves at the beginning of a call

B. Obtain written consent from potential customers
C. Register with the state before conducting business
D. Provide written contracts for customer transactions
Answer: (SHOW ANSWER)
" For example, more than half the states require that telemarketers obtain a license or register with the state.39" Excerpt From: "IAPP_US_TB_US-Private-Sector-Privacy-3E_1.0." Apple Books.
"states may require that a written contract be created for certain transaction".
Excerpt From: "IAPP_US_TB_US-Private-Sector-Privacy-3E_1.0." Apple Books.

NEW QUESTION: 58
The Video Privacy Protection Act of 1988 restricted which of the following?
A. Which purchase records of audio visual materials may be disclosed
B. When downloading of copyrighted audio visual materials is allowed
C. When a user's viewing of online video content can be monitored
D. Who advertisements for videos and video games may target
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://searchcompliance.techtarget.com/definition/Video-Privacy-Protection-Act-of-1988

NEW QUESTION: 59
Under the California Consumer Privacy Act (as amended by the California Pnvacy Rights Act), a consumer may Initiate a civil action against a business for?
A. Any personal information that is subject to unauthorized access or disclosure.
B. A security breach of certain categories of personal information that is nonencrypted and nonredacted
C. Failure to implement and maintain reasonable security procedures and practices to protect the personal information held.
D. Failure to implement and maintain security practices set out in regulations issued by the California Privacy Protection Agency (CPPA).
Answer: (SHOW ANSWER)
Under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), consumers have the right to initiate a civil action if a business fails to adequately protect their personal information and a security breach occurs. This right applies specifically to breaches of certain categories of personal information that are unencrypted and unredacted.
Key Details of CCPA/CPRA Civil Actions:
* Security Breaches:
* A consumer can sue a business if the breach involves personal information such as Social Security numbers, driver's license numbers, or financial account information, provided that the data was unencrypted and unredacted.

* Reasonable Security Practices:
* Businesses are required to implement and maintain reasonable security practices to protect personal information. Failure to do so may expose the business to liability in case of a breach.
* Categories of Data Covered:
* The law specifies that only certain sensitive categories of personal information are actionable under a civil suit.
Explanation of Options:
* A. Any personal information that is subject to unauthorized access or disclosure:This is incorrect.
The civil action is limited to specific sensitive data categories, not all personal information.
* B. A security breach of certain categories of personal information that is nonencrypted and nonredacted:This is correct. Civil actions under the CCPA/CPRA apply to breaches involving specific sensitive data that is not encrypted or redacted.
* C. Failure to implement and maintain reasonable security procedures and practices to protect the personal information held:While this is a requirement under the law, it does not by itself provide grounds for a civil action. A security breach must occur for a consumer to sue.
* D. Failure to implement and maintain security practices set out in regulations issued by the California Privacy Protection Agency (CPPA):This is incorrect. Civil actions are tied to breaches of sensitive data, not a failure to meet specific agency guidelines.
References from CIPP/US Materials:
* CCPA/CPRA (Civil Code § 1798.150): Outlines the private right of action for security breaches involving certain unencrypted and unredacted data.
* IAPP CIPP/US Certification Textbook: Discusses the conditions under which consumers may bring civil actions under the CCPA/CPRA.

NEW QUESTION: 60
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: B (LEAVE A REPLY)

NEW QUESTION: 61
Which jurisdiction must courts have in order to hear a particular case?
A. Subject matter jurisdiction and regulatory jurisdiction
B. Subject matter jurisdiction and professional jurisdiction

C. Personal jurisdiction and subject matter jurisdiction
D. Personal jurisdiction and professional jurisdiction
Answer: C (LEAVE A REPLY)
In order for a court to hear a case, it must have both personal jurisdiction and subject matter jurisdiction. Personal jurisdiction refers to the authority of a court over the parties to a case, while subject matter jurisdiction refers to the authority of a court to hear a particular type of case. For example, a federal court may have subject matter jurisdiction over a case involving a federal law, but it may not have personal jurisdiction over a defendant who has no contacts with the state where the court is located. Similarly, a state court may have personal jurisdiction over a resident of the state, but it may not have subject matter jurisdiction over a case involving a foreign treaty.

NEW QUESTION: 62
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: (SHOW ANSWER)

Data flow diagrams are graphical representations of how data moves within an organization or between different entities. They can help identify the sources, destinations, and processing of personal data, as well as the legal basis, retention periods, and security measures for each data flow. Reviewing the available data flow diagrams can help the data privacy leader to quickly and accurately respond to the urgent request from the EU-based retail partner, as well as to assess the potential risks and compliance gaps in the data transfer process. Data flow diagrams are also a key component of data protection impact assessments (DPIAs), which are required by the GDPR for high-risk processing activities.

NEW QUESTION: 63

SCENARIO

Please use the following to answer the next QUESTION

Noah is trying to get a new job involving the management of money. He has a poor personal credit rating, but he has made better financial decisions in the past two years. One potential employer, Arnie's Emporium, recently called to tell Noah he did not get a position. As part of the application process, Noah signed a consent form allowing the employer to request his credit report from a consumer reporting agency (CRA). Noah thinks that the report hurt his chances, but believes that he may not ever know whether it was his credit that cost him the job. However, Noah is somewhat relieved that he was not offered this particular position. He noticed that the store where he interviewed was extremely disorganized. He imagines that his credit report could still be sitting in the office, unsecured.

Two days ago, Noah got another interview for a position at Sam's Market. The interviewer told Noah that his credit report would be a factor in the hiring decision. Noah was surprised because he had not seen anything on paper about this when he applied.

Regardless, the effect of Noah's credit on his employability troubles him, especially since he has tried so hard to improve it. Noah made his worst financial decisions fifteen years ago, and they led to bankruptcy. These were decisions he made as a young man, and most of his debt at the time consisted of student loans, credit card debt, and a few unpaid bills - all of which Noah is still working to pay off. He often laments that decisions he made fifteen years ago are still affecting him today.

In addition, Noah feels that an experience investing with a large bank may have contributed to his financial troubles. In 2007, in an effort to earn money to help pay off his debt, Noah talked to a customer service representative at a large investment company who

urged him to purchase stocks. Without understanding the risks, Noah agreed. Unfortunately, Noah lost a great deal of money.
After losing the money, Noah was a customer of another financial institution that suffered a large security breach. Noah was one of millions of customers whose personal information was compromised. He wonders if he may have been a victim of identity theft and whether this may have negatively affected his credit.
Noah hopes that he will soon be able to put these challenges behind him, build excellent credit, and find the perfect job.
Based on the scenario, which legislation should ease Noah's worry about his credit report as a result of applying at Arnie's Emporium?
A. The Privacy Rule under the Gramm-Leach-Bliley Act (GLBA).
B. The Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA).
C. The Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA).
D. The Red Flags Rule under the Fair and Accurate Credit Transactions Act (FACTA).
Answer: C (LEAVE A REPLY)
The Department of Commerce (DOC) plays a role in privacy policy by promoting the development and adoption of voluntary codes of conduct, standards, and best practices for the private sector, as well as facilitating cross-border data transfers through mechanisms such as the EU-U.S. Privacy Shield and the APEC Cross-Border Privacy Rules. However, the DOC does not have regulatory authority to enforce privacy laws or impose sanctions for privacy violations. The other agencies listed have some degree of regulatory authority over privacy issues within their respective domains. For example, the Office of the Comptroller of the Currency (OCC) supervises national banks and federal savings associations and enforces the GLBA privacy and security rules for these institutions. The Federal Communications Commission (FCC) regulates interstate and international communications and enforces the privacy and security rules for telecommunications carriers, broadband providers, and voice over internet protocol (VoIP) services. The Department of Transportation (DOT) oversees the transportation sector and enforces the privacy and security rules for airlines, travel agents, and other covered entities under the Aviation and Transportation Security Act (ATSA). References:
* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 1: Introduction to the
U.S. Privacy Environment, Section 1.3: Federal Agencies with a Role in Privacy, p. 18-19
* IAPP CIPP/US Body of Knowledge, Domain I: Introduction to the U.S. Privacy Environment, Objective I.B: Identify the major federal agencies with a role in privacy, Subobjective I.B.4: Identify the role of the Department of Commerce, p. 7
* IAPP CIPP/US Exam Blueprint, Domain I: Introduction to the U.S. Privacy Environment, Objective I.
B: Identify the major federal agencies with a role in privacy, Subobjective I.B.4: Identify the role of the Department of Commerce, p. 3

NEW QUESTION: 64
Which of the following describes the most likely risk for a company developing a privacy policy with standards that are much higher than its competitors?
A. Getting accused of discriminatory practices
B. Having a security system failure
C. Being more closely scrutinized for any breaches of policy
D. Attracting skepticism from auditors
Answer: C (LEAVE A REPLY)

NEW QUESTION: 65
Which of the following is an example of federal preemption?
A. The Payment Card Industry's (PCI) ability to self-regulate and enforce data security standards for payment card data.
B. The U.S. Federal Trade Commission's (FTC) ability to enforce against unfair and deceptive trade practices across sectors and industries.
C. The California Consumer Privacy Act (CCPA) regulating businesses that have no physical brick- and- mortal presence in California, but which do business there.
D. The U.S. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act prohibiting states from passing laws that impose greater obligations on senders of email marketing.
Answer: D (LEAVE A REPLY)
Federal preemption is a doctrine in law that allows a federal law to take precedence over or to displace a state law in certain matters of national importance (such as interstate commerce). The doctrine is based on the Supremacy Clause of the Constitution, which declares that federal law is the "supreme law of the land" and that state judges are bound by it. There are two types of federal preemption: express and implied. Express preemption occurs when Congress expressly states that a federal law is intended to preempt certain types of state legislation. Implied preemption occurs when a state law conflicts with federal law because it is impossible to comply with both at the same time, or because it interferes with the objectives of the federal law, or because the federal government has fully occupied the field of regulation. The U.S. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act is an example of express preemption. The Act regulates commercial email messages and establishes requirements for senders and penalties for violations. The Act also explicitly preempts any state law that "expressly regulates the use of electronic mail to send commercial messages", except for state laws that prohibit falsity or deception. This means that states cannot pass laws that impose greater obligations on senders of email marketing than the federal law, such as requiring opt-in consent or providing additional opt-out mechanisms. Therefore, the CAN-SPAM Act is the correct answer to the question.

NEW QUESTION: 66

Which of the following best describes the ASIA-Pacific Economic Cooperation (APEC) principles?
A. An international court ruling on personal information held in the commercial sector.
B. A code of responsibilities for medical establishments to uphold privacy laws.
C. A bill of rights for individuals seeking access to their personal information.
D. A baseline of marketers' minimum responsibilities for providing opt-out mechanisms.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which federal agency plays a role in privacy policy, but does NOT have regulatory authority?
A. The Office of the Comptroller of the Currency.
B. The Federal Communications Commission.
C. The Department of Transportation.
D. The Department of Commerce.
Answer: D (LEAVE A REPLY)
The Department of Commerce (DOC) plays a role in privacy policy by promoting the development and adoption of voluntary codes of conduct, standards, and best practices for the private sector, as well as facilitating cross-border data transfers through mechanisms such as the EU-U.S. Privacy Shield and the APEC Cross-Border Privacy Rules. However, the DOC does not have regulatory authority to enforce privacy laws or impose sanctions for privacy violations. The other agencies listed have some degree of regulatory authority over privacy issues within their respective domains. For example, the Office of the Comptroller of the Currency (OCC) supervises national banks and federal savings associations and enforces the GLBA privacy and security rules for these institutions. The Federal Communications Commission (FCC) regulates interstate and international communications and enforces the privacy and security rules for telecommunications carriers, broadband providers, and voice over internet protocol (VoIP) services. The Department of Transportation (DOT) oversees the transportation sector and enforces the privacy and security rules for airlines, travel agents, and other covered entities under the Aviation and Transportation Security Act (ATSA). References:
* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 1: Introduction to the
U.S. Privacy Environment, Section 1.3: Federal Agencies with a Role in Privacy, p. 18-19
* IAPP CIPP/US Body of Knowledge, Domain I: Introduction to the U.S. Privacy Environment, Objective I.B: Identify the major federal agencies with a role in privacy, Subobjective I.B.4: Identify the role of the Department of Commerce, p. 7
* IAPP CIPP/US Exam Blueprint, Domain I: Introduction to the U.S. Privacy Environment, Objective I.
B: Identify the major federal agencies with a role in privacy, Subobjective I.B.4: Identify the role of the Department of Commerce, p. 3

NEW QUESTION: 68
Which law provides employee benefits, but often mandates the collection of medical information?
A. The Family and Medical Leave Act.
B. The Americans with Disabilities Act.
C. The Employee Medical Security Act.
D. The Occupational Safety and Health Act.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
The "Consumer Privacy Bill of Rights" presented in a 2012 Obama administration report is generally based on?
A. European Union Directive
B. The 1974 Privacy Act
C. Traditional fair information practices
D. Common law principles
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70
What was the primary reason for the creation of HIPAA?
A. To introduce protected health information security measures.
B. To increase the efficiency of electronic healthcare payments.
C. To create a common database within healthcare systems for patient diagnosis and prescription management.
D. To extend privacy laws to business associates within health care.
Answer: (SHOW ANSWER)
Although HIPAA contains extensive privacy protection, the law is mainly adopted to increase the efficiency of (electronic) healthcare payments.

NEW QUESTION: 71
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 (LEAVE A REPLY)

The scenario describes how the company had no adequate rules about access to customer information and how low-level employees had access to all of the company's customer data, including financial records. This indicates that the company did not implement proper access controls to limit who can access, use, or disclose customer information based on their roles and responsibilities. Access controls are one of the key elements of information security and privacy, as they help prevent unauthorized or inappropriate access to sensitive data.

Without access controls, the company's customer information was vulnerable to mishandling by employees or outsiders who could exploit the weak security measures. Therefore, the most likely cause of the breach was mishandling of information caused by lack of access controls. References:

* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4: Information Management from a U.S. Perspective, Section 4.2: Information Security, p. 113-114

* IAPP CIPP/US Body of Knowledge, Domain I: Introduction to the U.S. Privacy Environment, Objective I.C: Describe the role of information security in privacy, Subobjective I.C.1: Identify the key elements of information security, p. 8

NEW QUESTION: 72
How did the Fair and Accurate Credit Transactions Act (FACTA) amend the Fair Credit Reporting Act (FCRA)?
A. It expanded the definition of "consumer reports" to include communications relating to employee investigations
B. It required employers to get an employee's consent in advance of requesting a consumer report for internal investigation purposes Section: (none) Explanation
C. It increased the obligation of organizations to dispose of consumer data in ways that prevent unauthorized access
D. It stipulated the purpose of obtaining a consumer report can only be for a review of the employee's credit worthiness
Answer: C (LEAVE A REPLY)

NEW QUESTION: 73
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.
Under the GDPR, the complainant's request regarding her personal information is known as what?
A. Right of Access
B. Right of Removal

C. Right of Rectification
D. Right to Be Forgotten
Answer: D (LEAVE A REPLY)
Under the GDPR, the complainant's request regarding her personal information is known as the right to be forgotten, also known as the right to erasure. This right allows individuals to ask organizations to delete their personal data in certain circumstances, such as when the data is no longer necessary, the consent is withdrawn, or the processing is unlawful. The right to be forgotten is not absolute and may not apply if the processing is necessary for legal, public interest, or legitimate purposes. The right to be forgotten also requires organizations to inform any recipients of the data about the erasure request, unless it is impossible or involves disproportionate effort.

NEW QUESTION: 74
Which of the following best describes private-sector workplace monitoring in the United States?
A. Employers have broad authority to monitor their employees
B. U.S. federal law restricts monitoring only to industries for which it is necessary
C. Judgments in private lawsuits have severely limited the monitoring of employees
D. Most employees are protected from workplace monitoring by the U.S. Constitution
Answer: A (LEAVE A REPLY)
In the United States, there is no comprehensive federal law that regulates employee monitoring in the private sector. Instead, there are various federal and state laws that address specific aspects of monitoring, such as electronic communications, video surveillance, GPS tracking, and biometric data. Generally, these laws provide more protection for employees' privacy when they are using their own devices or personal accounts, or when they are outside of work hours or premises. However, when employees are using company-owned devices or accounts, or when they are performing work- related tasks, employers have broad authority to monitor their activities, as long as they have a legitimate business interest and do not violate any specific laws.
Employers are also advised to inform employees of their monitoring practices and obtain their consent, either explicitly or implicitly, to avoid potential legal disputes or employee backlash.

NEW QUESTION: 75
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?
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 (LEAVE A REPLY)

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 Virginiaresidents, 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.
References:
* [IAPP CIPP/US Study Guide], Chapter 10: State Data Security Laws, pp. 227-229.
* CIPP/US Practice Questions (Sample Questions), Question 32.

NEW QUESTION: 76
Which of the following most accurately describes the regulatory status ot pandemic contact-tracing apps in the United States?
A. Contact tracing is covered exclusively under the Health Insurance Portability and Accountability Act (HIPAA).
B. Contact tracing is regulated by the U.S. Centers for Disease Control and Prevention (CDC).
C. Contact tracing is subject to a patchwork of federal and state privacy laws
D. Contact tracing is not regulated in the United States.
Answer: C (LEAVE A REPLY)
In the United States, pandemic contact-tracing apps are regulated under a patchwork of federal and state privacy laws, rather than a single, comprehensive framework. Contact-tracing initiatives often involve the collection and processing of sensitive data, including location and health information, which may fall under different legal regimes depending on the jurisdiction and type of data.
Key Regulations Affecting Contact-Tracing Apps:
* State Privacy Laws:
* States such as California (via the California Consumer Privacy Act - CCPA) and others have privacy laws that may apply to contact-tracing apps, particularly when personal data is collected or shared.
* State-level health privacy laws may also govern how health-related data is collected and used.
* HIPAA:
* HIPAA (Health Insurance Portability and Accountability Act) applies only if the app is used by or on behalf of a covered entity (e.g., healthcare providers or health plans). If the app is operated by a private company without a connection to a HIPAA-covered entity, HIPAA likely does not apply.
* Federal Guidance:

* The Federal Trade Commission (FTC) enforces general privacy protections under Section 5 of the FTC Act, which prohibits unfair or deceptive practices.
* The FTC has also issued guidance on privacy considerations for health-related apps.
* Other Federal and Sector-Specific Laws:
* If the app collects health-related data, it could also trigger obligations under laws like the Americans with Disabilities Act (ADA) or sector-specific rules.
Explanation of Options:
* A. Contact tracing is covered exclusively under the Health Insurance Portability and Accountability Act (HIPAA):This is incorrect. HIPAA applies only to covered entities and their business associates, not broadly to all contact-tracing apps or initiatives.
* B. Contact tracing is regulated by the U.S. Centers for Disease Control and Prevention (CDC):
This is incorrect. While the CDC provides guidance and recommendations for public health, it does not have regulatory authority over contact-tracing apps.
* C. Contact tracing is subject to a patchwork of federal and state privacy laws:This is correct.
Contact-tracing apps in the U.S. are governed by various federal, state, and sector-specific laws, creating a patchwork regulatory framework.
* D. Contact tracing is not regulated in the United States:This is incorrect. While there is no single regulatory framework for contact tracing, the practice is subject to multiple federal and state laws.
References from CIPP/US Materials:
* IAPP CIPP/US Certification Textbook: Discusses the application of HIPAA, state privacy laws, and federal regulations to health-related technologies, including contact-tracing apps.
* FTC Guidance on Health Apps: Details privacy considerations for app developers handling health- related data.

NEW QUESTION: 77
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 a national origin

D. Questions about intended pregnancy

Answer: D (LEAVE A REPLY)

Title VII of the Civil Rights Act of 1964 is a federal law that prohibits employment discrimination based on race, color, religion, sex, and national origin1 It also prohibits retaliation against individuals who assert their rights under the law or participate in an EEOC investigation1 Title VII applies to employers with 15 or more employees, as well as to employment agencies, labor organizations, and joint labor-management committees1 Title VII prohibits employers from making pre-employment inquiries that express a preference, limitation, or specification based on any of the protected characteristics, unless they are bona fide occupational qualifications (BFOQs)2 BFOQs are rare and narrowly construed exceptions that allow employers to consider a protected characteristic when it is reasonably necessary to the normal operation of the business2 For example, a religious organization may require its employees to share its faith, or a women's shelter may hire only female counselors2 Option A is incorrect because questions about age are not prohibited by Title VII, but by the Age Discrimination in Employment Act of 1967 (ADEA), which protects individuals who are 40 years of age or older from employment discrimination based on age3 The ADEA generally prohibits employers from asking applicants about their age or date of birth, unless age is a BFOQ or the inquiry is part of a lawful affirmative action plan3 Option B is incorrect because questions about a disability are not prohibited by Title VII, but by the Americans with Disabilities Act of 1990 (ADA), which protects qualified individuals with disabilities from employment discrimination based on disability4 The ADA generally prohibits employers from asking applicants about whether they have a disability or the nature or severity of a disability, unless the inquiry is related to the ability to perform the essential functions of the job with or without reasonable accommodation4 Option C is incorrect because questions about a national origin are prohibited by Title VII, but not in all circumstances. Title VII prohibits employers from asking applicants about their national origin, ancestry, birthplace, native language, or accent, unless they are BFOQs or the inquiry is related to a legitimate business purpose, such as verifying eligibility to work in the United States or assessing language proficiency for a job that requires communication skills25 Option D is correct because questions about intended pregnancy are prohibited by Title VII, as amended by the Pregnancy Discrimination Act of 1978 (PDA), which protects women from employment discrimination based on pregnancy, childbirth, or related medical conditions. The PDA prohibits employers from asking applicants about whether they are pregnant or intend to become pregnant, unless they are related to the ability to perform the job. Such questions may indicate an intent to discriminate based on sex or pregnancy, or may deter women from applying for certain jobs.

References: 1: Title VII of the Civil Rights Act of 1964 | U.S. Equal Employment Opportunity Commission 2: Questions and Answers about Race and Color Discrimination in Employment | U.S. Equal Employment Opportunity Commission 3: Age Discrimination |

U.S. Equal Employment Opportunity Commission 4: Disability Discrimination | U.S. Equal Employment Opportunity Commission 5: National Origin Discrimination | U.S. Equal Employment Opportunity Commission : Pregnancy Discrimination | U.S. Equal Employment Opportunity Commission

NEW QUESTION: 78
How did the Fair and Accurate Credit Transactions Act (FACTA) amend the Fair Credit Reporting Act (FCRA)?
A. It expanded the definition of "consumer reports" to include communications relating to employee investigations
B. It increased the obligation of organizations to dispose of consumer data in ways that prevent unauthorized access
C. It stipulated the purpose of obtaining a consumer report can only be for a review of the employee's credit worthiness
D. It required employers to get an employee's consent in advance of requesting a consumer report for internal investigation purposes
Answer: B (LEAVE A REPLY)
FACTA added a new section to the FCRA that requires any person who maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose, to properly dispose of any such information or compilation. The purpose of this provision is to reduce the risk of identity theft and other consumer harm resulting from improper disposal of consumer information. The FTC and other federal agencies have issued rules implementing this provision, which specify the reasonable measures that covered entities must take to ensure secure disposal of consumer information, such as burning, pulverizing, shredding, erasing, or otherwise modifying the information to make it unreadable or indecipherable (16 CFR § 682.3).
References: 1, 2, 3

NEW QUESTION: 79
Which of the following best describes how federal anti-discrimination laws protect the privacy of private- sector employees in the United States?
A. They prescribe working environments that are safe and comfortable.
B. They limit the amount of time a potential employee can be interviewed.
C. They promote a workforce of employees with diverse skills and interests.
D. They limit the types of information that employers can collect about employees.
Answer: D (LEAVE A REPLY)
Federal anti-discrimination laws, such as Title VII of the Civil Rights Act of 1964, the Equal Pay Act of 1963, the Age Discrimination in Employment Act of 1967, and the Americans with Disabilities Act of 1990, prohibit employers from discriminating against employees or applicants based on certain protected characteristics, such as race, color, religion, sex, national origin, age, disability, and genetic information.

These laws also limit the types of information that employers can collect, use, disclose, or retain about employees or applicants, in order to prevent discrimination or invasion of privacy. For example, employers cannot ask about an applicant's medical history, disability status, genetic information, or religious beliefs, unless they are relevant to the job or a bona fide occupational qualification. Employers also cannot use such information to make adverse employment decisions, such as hiring, firing, promotion, or compensation, unless they are justified by a legitimate business necessity or a reasonable accommodation. Employers must also safeguard the confidentiality of such information and dispose of it properly when it is no longer needed. References:

* Federal Laws Prohibiting Job Discrimination Questions And Answers
* Laws Enforced by EEOC
* Employment and Anti-Discrimination Laws in the Workplace
* Protections Against Discrimination and Other Prohibited Practices
* 3. Who is protected from employment discrimination?

NEW QUESTION: 80

The Cable Communications Policy Act of 1984 requires which activity?

A. Obtaining subscriber consent for disseminating any personal information necessary to render cable services

B. Destruction of personal information a maximum of six months after it is no longer needed

C. Delivery of an annual notice detailing how subscriber information is to be used

D. Notice to subscribers of any investigation involving unauthorized reception of cable services

Answer: C (LEAVE A REPLY)

NEW QUESTION: 81

Under the California Consumer Privacy Act (as amended by the California Pnvacy Rights Act), a consumer may Initiate a civil action against a business for?

A. Any personal information that is subject to unauthorized access or disclosure.

B. A security breach of certain categories of personal information that is nonencrypted and nonredacted

C. Failure to implement and maintain reasonable security procedures and practices to protect the personal information held.

D. Failure to implement and maintain security practices set out in regulations issued by the California Privacy Protection Agency (CPPA).

Answer: B (LEAVE A REPLY)

Under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), consumers have the right to initiate a civil action if a business fails to adequately protect their personal information and a security breach occurs. This right

applies specifically to breaches of certain categories of personal information that are unencrypted and unredacted.
Key Details of CCPA/CPRA Civil Actions:
Security Breaches:
A consumer can sue a business if the breach involves personal information such as Social Security numbers, driver's license numbers, or financial account information, provided that the data was unencrypted and unredacted.
Reasonable Security Practices:
Businesses are required to implement and maintain reasonable security practices to protect personal information. Failure to do so may expose the business to liability in case of a breach.
Categories of Data Covered:
The law specifies that only certain sensitive categories of personal information are actionable under a civil suit.

NEW QUESTION: 82
SCENARIO
Please use the following to answer the next question:
Cheryl is the sole owner of Fitness Coach, Inc., a medium-sized company that helps individuals realize their physical fitness goals through classes, individual instruction, and access to an extensive indoor gym. She has owned the company for ten years and has always been concerned about protecting customer's privacy while maintaining the highest level of service. She is proud that she has built long-lasting customer relationships.
Although Cheryl and her staff have tried to make privacy protection a priority, the company has no formal privacy policy. So Cheryl hired Janice, a privacy professional, to help her develop one.
After an initial assessment, Janice created a first of a new policy. Cheryl read through the draft and was concerned about the many changes the policy would bring throughout the company. For example, the draft policy stipulates that a customer's personal information can only be held for one year after paying for a service such as a session with personal trainer. It also promises that customer information will not be shared with third parties without the written consent of the customer. The wording of these rules worry Cheryl since stored personal information often helps her company to serve her customers, even if there are long pauses between their visits. In addition, there are some third parties that provide crucial services, such as aerobics instructors who teach classes on a contract basis. Having access to customer files and understanding the fitness levels of their students helps instructors to organize their classes.
Janice understood Cheryl's concerns and was already formulating some ideas for revision. She tried to put Cheryl at ease by pointing out that customer data can still be kept, but that it should be classified according to levels of sensitivity. However, Cheryl was skeptical. It seemed that classifying data and treating each type differently would cause undue

difficulties in the company's day-to-day operations. Cheryl wants one simple data storage and access system that any employee can access if needed.
Even though the privacy policy was only a draft, she was beginning to see that changes within her company were going to be necessary. She told Janice that she would be more comfortable with implementing the new policy gradually over a period of several months, one department at a time. She was also interested in a layered approach by creating documents listing applicable parts of the new policy for each department.
What is the most likely risk of Fitness Coach, Inc. adopting Janice's first draft of the privacy policy?
A. Leaving the company susceptible to violations by setting unrealistic goals
B. Failing to meet the needs of customers who are concerned about privacy
C. Showing a lack of trust in the organization's privacy practices
D. Not being in standard compliance with applicable laws
Answer: A (LEAVE A REPLY)
Janice's first draft of the privacy policy may be too restrictive and impractical for Fitness Coach, Inc. to follow, given the nature of its business and the expectations of its customers. By limiting the retention of personal information to one year and requiring written consent for any third-party sharing, the policy may create operational challenges and customer dissatisfaction. For example, customers may want to resume their fitness programs after a long hiatus and expect the company to have their previous records and preferences. Similarly, third-party contractors may need access to customer information to provide better services and tailor their classes. If the company fails to adhere to its own privacy policy, it may face legal consequences, reputational damage, and loss of trust from its customers. Therefore, the company should adopt a more realistic and flexible privacy policy that balances its business needs and its customers' privacy rights.

NEW QUESTION: 83
The rules for "e-discovery" mainly prevent which of the following?
A. A conflict between business practice and technological safeguards
B. The loss of information due to poor data retention practices
C. The practice of employees using personal devices for work
D. A breach of an organization's data retention program
Answer: A (LEAVE A REPLY)
E-discovery is the process by which parties share, review, and collect electronically stored information (ESI) to use as evidence in a legal matter. The rules for e-discovery mainly prevent a conflict between business practice and technological safeguards, because they establish the standards and procedures for preserving, collecting, reviewing, and producing ESI in a way that balances the needs of litigation with the realities of technology. For example, the Federal Rules of Civil Procedure (FRCP) provide guidance on the scope, timing, format, and methods of e- discovery, as well as the sanctions for failing to comply with e-discovery obligations. The rules also encourage cooperation and communication

among parties and courts to resolve e-discovery issues efficiently and effectively. By following the rules for e-discovery, parties can avoid disputes, delays, and costs that may arise from incompatible or inconsistent business and technological practices.

NEW QUESTION: 84
SCENARIO
Please use the following to answer the next question:
Cheryl is the sole owner of Fitness Coach, Inc., a medium-sized company that helps individuals realize their physical fitness goals through classes, individual instruction, and access to an extensive indoor gym. She has owned the company for ten years and has always been concerned about protecting customer's privacy while maintaining the highest level of service. She is proud that she has built long-lasting customer relationships.
Although Cheryl and her staff have tried to make privacy protection a priority, the company has no formal privacy policy. So Cheryl hired Janice, a privacy professional, to help her develop one.
After an initial assessment, Janice created a first of a new policy. Cheryl read through the draft and was concerned about the many changes the policy would bring throughout the company. For example, the draft policy stipulates that a customer's personal information can only be held for one year after paying for a service such as a session with personal trainer. It also promises that customer information will not be shared with third parties without the written consent of the customer. The wording of these rules worry Cheryl since stored personal information often helps her company to serve her customers, even if there are long pauses between their visits. In addition, there are some third parties that provide crucial services, such as aerobics instructors who teach classes on a contract basis. Having access to customer files and understanding the fitness levels of their students helps instructors to organize their classes.
Janice understood Cheryl's concerns and was already formulating some ideas for revision. She tried to put Cheryl at ease by pointing out that customer data can still be kept, but that it should be classified according to levels of sensitivity. However, Cheryl was skeptical. It seemed that classifying data and treating each type differently would cause undue difficulties in the company's day-to-day operations. Cheryl wants one simple data storage and access system that any employee can access if needed.
Even though the privacy policy was only a draft, she was beginning to see that changes within her company were going to be necessary. She told Janice that she would be more comfortable with implementing the new policy gradually over a period of several months, one department at a time. She was also interested in a layered approach by creating documents listing applicable parts of the new policy for each department.
Based on the scenario, which of the following would have helped Janice to better meet the company's needs?
A. Creating a more comprehensive plan for implementing a new policy
B. Spending more time understanding the company's information goals

C. Explaining the importance of transparency in implementing a new policy
D. Removing the financial burden of the company's employee training program
Answer: B (LEAVE A REPLY)
According to the Wiley study guide, one of the steps in developing a privacy policy is to conduct a privacy assessment, which involves identifying the organization's information goals and needs, as well as the legal and regulatory requirements that apply to its data collection and use practices.
By spending more time understanding the company's information goals, Janice would have been able to tailor the privacy policy to fit the company's business model and customer expectations, while still complying with the relevant privacy laws and standards. This would have also helped Janice to address Cheryl's concerns about the impact of the policy on the company's operations and customer relationships, and to propose solutions that balance privacy protection and service delivery.

NEW QUESTION: 85
When developing a company privacy program, which of the following relationships will most help a privacy professional develop useful guidance for the organization?
A. Relationships with individuals within the privacy professional community who are able to share expertise and leading practices for different industries.
B. Relationships with clients, vendors, and customers whose data will be primarily collected and used throughout the organizational program.
C. Relationships with company leaders responsible for approving, implementing, and periodically reviewing the corporate privacy program.
D. Relationships with individuals across company departments and at different levels in the organization's hierarchy.
Answer: D (LEAVE A REPLY)
When developing a company privacy program, a privacy professional needs to understand the business objectives, processes, and risks of the organization, as well as the legal and regulatory requirements and best practices for privacy. To achieve this, a privacy professional should establish and maintain relationships with individuals across company departments and at different levels in the organization's hierarchy, such as IT, marketing, human resources, legal, compliance, security, and senior management. These relationships will help the privacy professional to gather relevant information, identify privacy issues and gaps, communicate privacy policies and procedures, provide training and awareness, monitor compliance, and resolve conflicts. The other relationships listed are also important, but not as essential as the internal relationships for developing a company privacy program.

NEW QUESTION: 86
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 (LEAVE A REPLY)
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.

NEW QUESTION: 87
When developing a company privacy program, which of the following relationships will most help a privacy professional develop useful guidance for the organization?
A. Relationships with individuals within the privacy professional community who are able to share expertise and leading practices for different industries.
B. Relationships with clients, vendors, and customers whose data will be primarily collected and used throughout the organizational program.
C. Relationships with company leaders responsible for approving, implementing, and periodically reviewing the corporate privacy program.
D. Relationships with individuals across company departments and at different levels in the organization's hierarchy.
Answer: D (LEAVE A REPLY)
IAPP Book, Section 4.3.1.1, paragraph 3.

NEW QUESTION: 88
Which of the following is an example of federal preemption?
A. The U.S. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act prohibiting states from passing laws that impose greater obligations on senders of email marketing.
B. The U.S. Federal Trade Commission's (FTC) ability to enforce against unfair and deceptive trade practices across sectors and industries.
C. The Payment Card Industry's (PCI) ability to self-regulate and enforce data security standards for payment card data.
D. The California Consumer Privacy Act (CCPA) regulating businesses that have no physical brick-and-mortal presence in California, but which do business there.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
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 (LEAVE A REPLY)
The most likely reason that states have adopted their own data breach notification laws is that many types of organizations are not currently subject to federal laws regarding breaches. As explained in the Data Breach Response: A Guide for Business from the Federal Trade Commission (FTC), certain federal laws govern obligations to report data breaches in particular industries, such as health care, financial services, or telecommunications. However, these laws do not cover all types of businesses or all types of personal information that may be compromised in a data breach. Therefore, states have enacted their own data breach notification laws to fill the gaps and protect the privacy and security of their residents. According to the National Conference of State Legislatures, as of January 2022, all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. These state laws vary in terms of the definitions of personal information, the triggers for notification, the methods and timing of notification, the exemptions and exceptions, and the penalties and enforcement mechanisms.

NEW QUESTION: 90
Which of the following laws is NOT involved in the regulation of employee background checks?
A. The Civil Rights Act.
B. The Gramm-Leach-Bliley Act (GLBA).
C. The U.S. Fair Credit Reporting Act (FCRA).
D. The California Investigative Consumer Reporting Agencies Act (ICRAA).
Answer: B (LEAVE A REPLY)
The law that is not involved in the regulation of employee background checks is B. The Gramm-Leach-Bliley Act (GLBA). The GLBA is a federal law that regulates the privacy and security of financial information collected, used, or shared by financial institutions, such as banks, insurance companies, or securities firms.
The GLBA does not apply to employee background checks, unless the employer is a financial institution that obtains financial information from a consumer reporting agency for

employment purposes. In that case, the employer must comply with the GLBA's notice and opt-out requirements, as well as the FCRA's requirements for using consumer reports.
References:
* [IAPP CIPP/US Study Guide], Chapter 4: Workplace Privacy, pp. 113-114.
* IAPP CIPP/US Body of Knowledge, Section IV: Workplace Privacy, Subsection A: Employee Privacy Expectations, Topic 3: Background Checks.
* IAPP CIPP/US Practice Questions, Question 150.

NEW QUESTION: 91
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 Asi a. 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 Station's network and was able to steal data relating to employees in the company'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. Obtain express consent from employees for storing the HR data in the cloud and keep a record of the employee consents.
B. Negotiate a Business Associate Agreement with the cloud provider to protect any health-related data employees might share with Filtration Station.
C. Request that the Board sign off in a written document on the choice of cloud provider.
D. Ensure that the cloud provider abides by the contractual requirements by conducting an on-site audit.
Answer: (SHOW ANSWER)

NEW QUESTION: 92
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?
A. Honored the promise of its privacy policy to acquire information by using an opt-in method.

B. Communicated requests for changes to users' preferences across the organization and with third parties.
C. Implemented a comprehensive policy for accessing customer information.
D. Looked for any persistent threats to security that could compromise the company's network.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 93
Which was NOT one of the five priority areas listed by the Federal Trade Commission in its 2012 report,
"Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"?
A. International data transfers
B. Large platform providers
C. Promoting enforceable self-regulatory codes
D. Do Not Track
Answer: D (LEAVE A REPLY)
The Federal Trade Commission (FTC) issued its 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"1, which outlined a framework for privacy protection based on three main principles: privacy by design, simplified consumer choice, and greater transparency. The report also identified five priority areas for the FTC's privacy enforcement and policy efforts, which were:
* Data brokers
* Large platform providers
* Mobile
* Promoting enforceable self-regulatory codes
* International data transfers
Do Not Track was not one of the five priority areas, but rather a specific mechanism for implementing the principle of simplified consumer choice. The report endorsed the development of a Do Not Track system that would allow consumers to opt out of online behavioral advertising across websites and platforms1. The report also noted the progress made by various stakeholders, such as the World Wide Web Consortium (W3C), the Digital Advertising Alliance (DAA), and browser companies, in advancing the Do Not Track initiative1. References: 1: Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012), available at 1.

NEW QUESTION: 94
Which of the following privacy rights is NOT available under the Colorado Privacy Act?
A. The right to access sensitive data.

B. The right to correct sensitive data.
C. The right to delete sensitive data.
D. The right to limit the use of sensitive data.
Answer: D (LEAVE A REPLY)
"The CPA grants Colorado Consumers new rights with respect to their personal data, including the right to access, delete, and correct their personal data as well as the right to opt out of the sale of their personal data or its use for targeted advertising or certain kinds of profiling."
https://coag.gov/resources/colorado-privacy-act/
Even without knowing for certain the answer, one can reason that it should be D. It would be administratively difficult for businesses to adhere to varying limitation requests for each consumer... Therefore such a right would not make sense from a public policy perspective.

NEW QUESTION: 95
If an organization maintains data classified as high sensitivity in the same system as data classified as low sensitivity, which of the following is the most likely outcome?
A. The organization will still be in compliance with most sector-specific privacy and security laws.
B. The impact of an organizational data breach will be more severe than if the data had been segregated.
C. Temporary employees will be able to find the data necessary to fulfill their responsibilities.
D. The organization will be able to address legal discovery requests efficiently without producing more information than necessary.
Answer: (SHOW ANSWER)
Data classification is the process of categorizing data based on its sensitivity and importance to determine its level of confidentiality and protection. Data classification helps organizations apply appropriate security and compliance measures to ensure each category receives proper protection. Data classification also helps organizations identify which data is subject to specific privacy laws and regulations, such as the GDPR, HIPAA, or CCPA, and how to handle data subject requests, data breaches, or legal discovery. If an organization maintains data classified as high sensitivity, such as personal information, financial information, or health information, in the same system as data classified as low sensitivity, such as public information or internal information, it increases the risk of exposing the high sensitivity data in the event of a data breach. A data breach can result in legal consequences, reputational damage, and loss of trust from customers and stakeholders. Therefore, it is advisable to segregate data based on its classification and apply different levels of encryption, access control, and monitoring to each category. This way, the organization can minimize the impact of a data breach and protect the privacy and security of its data assets.

NEW QUESTION: 96
According to FERPA, when can a school disclose records without a student's consent?
A. If the disclosure is not to be conducted through email to the third party
B. If the disclosure would not reveal a student's student identification number
C. If the disclosure is to practitioners who are involved in a student's health care
D. If the disclosure is to provide transcripts to a school where a student intends to enroll
Answer: D (LEAVE A REPLY)
According to FERPA, a school may disclose personally identifiable information (PII) from an eligible student's education records without consent if the disclosure meets one of the exceptions in 34 CFR § 99.31.
One of these exceptions is for disclosures to other schools to which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer (34 CFR § 99.31(a)(2)). This exception allows schools to disclose transcripts, recommendations, or other information that may facilitate the student's admission or enrollment at another school. However, the school must make a reasonable attempt to notify the student of the disclosure, unless the student initiated the disclosure, and must provide the student with a copy of the records that were disclosed upon request (34 CFR § 99.34(a)(1)). References: https://studentprivacy.ed.gov/ferpa https://studentprivacy.ed.gov/ferpa

NEW QUESTION: 97
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 (LEAVE A REPLY)
The Red Flag Program Clarification Act of 2010 amended the original Red Flags rule, which required certain financial institutions and creditors to develop and implement a written identity theft prevention program. The Clarification Act narrowed the definition of creditor to include only those who regularly and in the ordinary course of business advance funds to or on behalf of aperson, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person12. This excludes creditors who advance funds for expenses incidental to a service provided by the creditor to that person3. References:
* CIPP/US Practice Questions (Sample Questions), Question 133, Answer B, Explanation B.
* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4, Section 4.3, p.108-109.

* Red Flag Program Clarification Act of 2010, Section 2, Subsection (b).

NEW QUESTION: 98
All of the following common law torts are relevant to employee privacy under US law EXCEPT?
A. Intrusion upon seclusion.
B. Infliction of emotional distress.
C. Defamation
D. Conversion.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99
What is the main purpose of the Global Privacy Enforcement Network?
A. To promote universal cooperation among privacy authorities
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: (SHOW ANSWER)
The Global Privacy Enforcement Network (GPEN) is a network for privacy enforcement authorities (PEAs) to share knowledge, experience and best practices on the practical aspects of privacy enforcement and cooperation. GPEN was created in response to the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, which called for member countries to foster the establishment of an informal network of PEAs. GPEN's main purpose is to facilitate cross-border cooperation and coordination among PEAs, especially in cases involving multiple jurisdictions or regions. GPEN also aims to enhance information sharing, promote awareness and education, and support capacity building among PEAs. References:
* Home (public) | Global Privacy Enforcement Network
* Global Privacy Enforcement Network - International Association of Privacy Professionals
* International Partnerships - Office of the Privacy Commissioner of Canada
* Specialised networks - Global Privacy Assembly
* Action Plan for the Global Privacy Enforcement Network (GPEN)
* [IAPP CIPP/US Certified Information Privacy Professional Study Guide], Chapter 6, page 213.

NEW QUESTION: 100
Which of the following types of information would an organization generally NOT be required to disclose to law enforcement?
A. Information about workspace injuries under OSHA requirements
B. Personal health information under the HIPAA Privacy Rule
C. Information about medication errors under the Food, Drug and Cosmetic Act

D. Money laundering information under the Bank Secrecy Act of 1970
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
How did the Fair and Accurate Credit Transactions Act (FACTA) amend the Fair Credit Reporting Act (FCRA)?
A. It expanded the definition of "consumer reports" to include communications relating to employee investigations
B. It increased the obligation of organizations to dispose of consumer data in ways that prevent unauthorized access
C. It stipulated the purpose of obtaining a consumer report can only be for a review of the employee's credit worthiness
D. It required employers to get an employee's consent in advance of requesting a consumer report for internal investigation purposes
Answer: B (LEAVE A REPLY)
FACTA added a new section to the FCRA that requires any person who maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose, to properly dispose of any such information or compilation. The purpose of this provision is to reduce the risk of identity theft and other consumer harm resulting from improper disposal of consumer information. The FTC and other federal agencies have issued rules implementing this provision, which specify the reasonable measures that covered entities must take to ensure secure disposal of consumer information, such as burning, pulverizing, shredding, erasing, or otherwise modifying the information to make it unreadable or indecipherable (16 CFR ?682.3).

NEW QUESTION: 102
Which was NOT one of the five priority areas listed by the Federal Trade Commission in its 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"?
A. International data transfers
B. Large platform providers
C. Promoting enforceable self-regulatory codes
D. Do Not Track
Answer: D (LEAVE A REPLY)
The Federal Trade Commission (FTC) issued its 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"1, which outlined a framework for privacy protection based on three main principles: privacy by design, simplified consumer choice, and greater transparency. The report also identified five priority areas for the FTC's privacy enforcement and policy efforts, which were:
Data brokers

Large platform providers
Mobile
Promoting enforceable self-regulatory codes
International data transfers
Do Not Track was not one of the five priority areas, but rather a specific mechanism for implementing the principle of simplified consumer choice. The report endorsed the development of a Do Not Track system that would allow consumers to opt out of online behavioral advertising across websites and platforms. The report also noted the progress made by various stakeholders, such as the World Wide Web Consortium (W3C), the Digital Advertising Alliance (DAA), and browser companies, in advancing the Do Not Track initiative.

NEW QUESTION: 103
SCENARIO
Please use the following to answer the next question:
You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in statea. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo.
CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.
A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals ?ones that exposed the PHI of public figures including celebrities and politicians.
During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.
A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.

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

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

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

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

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

Answer: B (LEAVE A REPLY)

The HIPAA privacy rule establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information") and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (collectively defined as

"covered entities")1 The rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization1 The rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections1 The HIPAA privacy rule permits a covered entity to disclose protected health information for the litigation in response to a court order, subpoena, discovery request, or other lawful process, provided the applicable requirements of 45 CFR 164.512 (e) for disclosures for judicial and administrative proceedings are met. These requirements include:

In response to a court order or administrative tribunal order, the covered entity may disclose only the protected health information expressly authorized by such order. In response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order or administrative tribunal order, the covered entity must receive satisfactory assurances that the party seeking the information has made reasonable efforts to ensure that the individual who is the subject of the information has been given notice of the request, or that the party seeking the information has made reasonable efforts to secure a qualified protective order. A qualified protective order is an order of a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested and requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

NEW QUESTION: 104

What type of material is exempt from an individual's right to disclosure under the Privacy Act?
A. Material requires by statute to be maintained and used solely for research purposes.
B. Material reporting investigative efforts to prevent unlawful persecution of an individual.
C. Material used to determine potential collaboration with foreign governments in negotiation of trade deals.
D. Material reporting investigative efforts pertaining to the enforcement of criminal law.
Answer: B (LEAVE A REPLY)
https://www.dea.gov/foia/privacy-act-exemptions

NEW QUESTION: 105
Which federal act does NOT contain provisions for preempting stricter state laws?
A. The CAN-SPAM Act
B. The Children's Online Privacy Protection Act (COPPA)
C. The Fair and Accurate Credit Transactions Act (FACTA)
D. The Telemarketing Consumer Protection and Fraud Prevention Act
Answer: D (LEAVE A REPLY)
The federal act that does NOT contain provisions for preempting stricter state laws is the Telemarketing Consumer Protection and Fraud Prevention Act. This act authorizes the Federal Trade Commission (FTC) to establish and enforce rules for telemarketing practices, such as the Do Not Call Registry, the prohibition of robocalls, and the disclosure of material information.
However, the act also explicitly states that it does not "annul, alter, or affect, or exempt any person subject to the provisions of this section from complying with, the laws of any State with respect to telemarketing practices, except to the extent that those laws are inconsistent with any provision of this section, and then only to the extent of the inconsistency". This means that states can enact and enforce their own laws regarding telemarketing, as long as they are not less protective than the federal law. In contrast, the other three acts listed in the question do contain preemption clauses that limit or override the authority of states to regulate certain aspects of electronic communications, online privacy, and credit transactions.

NEW QUESTION: 106
If an organization maintains data classified as high sensitivity in the same system as data classified as low sensitivity, which of the following is the most likely outcome?
A. The organization will still be in compliance with most sector-specific privacy and security laws.
B. The impact of an organizational data breach will be more severe than if the data had been segregated.
C. Temporary employees will be able to find the data necessary to fulfill their responsibilities.

D. The organization will be able to address legal discovery requests efficiently without producing more information than necessary.

Answer: (SHOW ANSWER)

Data classification is the process of categorizing data based on its sensitivity and importance to determine its level of confidentiality and protection. Data classification helps organizations apply appropriate security and compliance measures to ensure each category receives proper protection1. Data classification also helps organizations identify which data is subject to specific privacylaws and regulations, such as the GDPR, HIPAA, or CCPA, and how to handle data subject requests, data breaches, or legal discovery2. If an organization maintains data classified as high sensitivity, such as personal information, financial information, or health information, in the same system as data classified as low sensitivity, such as public information or internal information, it increases the risk of exposing the high sensitivity data in the event of a data breach. A data breach can result in legal consequences, reputational damage, and loss of trust from customers and stakeholders. Therefore, it is advisable to segregate data based on its classification and apply different levels of encryption, access control, and monitoring to each category3. This way, the organization can minimize the impact of a data breach and protect the privacy and security of its data assets. References:

* Why Is Data Classification Important?
* Data Classification for GDPR Explained
* Data classification and privacy considerations

NEW QUESTION: 107

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

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

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

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

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

Answer: (SHOW ANSWER)
The Dodd-Frank Act created the Consumer Financial Protection Bureau (CFPB) as an independent agency within the Federal Reserve System. The CFPB has the authority to regulate consumer financial products and services, such as mortgages, credit cards, student loans, and payday loans. One of the main objectives of the CFPB is to promote transparency, fairness, and consumer choice in the financial marketplace. The CFPB has issued rules and guidance to require financial institutions to provide clear and accurate information to consumers about the costs, risks, and benefits of their products and services. The CFPB also has the power to enforce consumer protection laws and prohibit unfair, deceptive, or abusive acts or practices by financial institutions123 References: 1: Dodd-Frank Wall Street Reform and Consumer Protection Act, Title X, Subtitle A, Section 1011. 2: Consumer Financial Protection Bureau, Wikipedia. 3: Dodd-Frank Act: What It Does, Major Components, and Criticisms, Investopedia.

NEW QUESTION: 108
Which venture would be subject to the requirements of Section 5 of the Federal Trade Commission Act?
A. A city bus system's frequent rider program
B. A national bank's no-fee checking promotion
C. An online merchant's free shipping offer
D. A local nonprofit charity's fundraiser
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Which of the following describes the most likely risk for a company developing a privacy policy with standards that are much higher than its competitors?
A. Being more closely scrutinized for any breaches of policy
B. Getting accused of discriminatory practices
C. Attracting skepticism from auditors
D. Having a security system failure
Answer: (SHOW ANSWER)
A company that develops a privacy policy with standards that are much higher than its competitors may face the risk of being more closely scrutinized for any breaches of policy by regulators, customers, media, or other stakeholders. This is because the company sets a higher expectation for its privacy practices and may be held to a higher standard of accountability and transparency. If the company fails to comply with its own policy or experiences a data breach, it may face more severe consequences, such as reputational damage, loss of trust, legal liability, or regulatory sanctions. References:
* IAPP CIPP/US Body of Knowledge, Section I, B, 2
* [IAPP CIPP/US Study Guide, Chapter 1, Section 1.4]

NEW QUESTION: 110
Which of the following best describes private-sector workplace monitoring in the United States?
A. Employers have broad authority to monitor their employees
B. U.S. federal law restricts monitoring only to industries for which it is necessary
C. Judgments in private lawsuits have severely limited the monitoring of employees
D. Most employees are protected from workplace monitoring by the U.S. Constitution
Answer: A (LEAVE A REPLY)
In the United States, there is no comprehensive federal law that regulates employee monitoring in the private sector. Instead, there are various federal and state laws that address specific aspects of monitoring, such as electronic communications, video surveillance, GPS tracking, and biometric data. Generally, these laws provide more protection for employees' privacy when they are using their own devices or personal accounts, or when they are outside of work hours or premises. However, when employees are using company-owned devices or accounts, or when they are performing work-related tasks, employers have broad authority to monitor their activities, as long as they have a legitimate business interest and do not violate any specific laws. Employers are also advised to inform employees of their monitoring practices and obtain their consent, either explicitly or implicitly, to avoid potential legal disputes or employee backlash123
References: https://www.jibble.io/article/us-employee-monitoring
https://www.worktime.com/most-asked-questions-on-us-employee-monitoring-laws

NEW QUESTION: 111
All of the following common law torts are relevant to employee privacy under US law EXCEPT?
A. Infliction of emotional distress.
B. Intrusion upon seclusion.
C. Defamation
D. Conversion.
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://en.wikipedia.org/wiki/Privacy_law

NEW QUESTION: 112
Under state breach notification laws, which is NOT typically included in the definition of personal information?
A. State identification number
B. First and last name
C. Social Security number
D. Medical Information
Answer: (SHOW ANSWER)

Under state breach notification laws, personal information is typically defined as an individual's first name or first initial and last name plus one or more other data elements, such as Social Security number, state identification number, account number, medical information, etc. However, first and last name alone are not usually considered personal information, unless they are combined with other data elements that could identify the individual or compromise their security or privacy. Therefore, option B is the correct answer, as it is not typically included in the definition of personal information under state breach notification laws. References: https://www.ncsl.org/technology-and-communication/security-breach-notification-lawshttps://

NEW QUESTION: 113
A law enforcement subpoenas the ACME telecommunications company for access to text message records of a person suspected of planning a terrorist attack. The company had previously encrypted its text message records so that only the suspect could access this data.
What law did ACME violate by designing the service to prevent access to the information by a law enforcement agency?
A. SCA
B. ECPA
C. CALEA
D. USA Freedom Act
Answer: C (LEAVE A REPLY)
The law that ACME violated by designing the service to prevent access to the information by a law enforcement agency is the Communications Assistance for Law Enforcement Act (CALEA)1. CALEA is a federal law that requires telecommunications carriers and manufacturers of telecommunications equipment to design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for interception of communications2. CALEA applies to all commercial messages, including text messages, and gives law enforcement agencies the authority to subpoena the records of such communications from the service providers3. By encrypting its text message records so that only the suspect could access this data, ACME violated CALEA's duty to cooperate in the interception of communications for law enforcement purposes. References: 1: Communications Assistance for Law Enforcement Act - Wikipedia2: Home | CALEA | The Commission on Accreditation for Law Enforcement Agencies, Inc.3: Communications Assistance for Law Enforcement Act : IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 6: Law Enforcement and National Security Access, p.
177

NEW QUESTION: 114
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.

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

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

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

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 115

What is an exception to the Electronic Communications Privacy Act of 1986 ban on interception of wire, oral and electronic communications?

A. Where one of the parties has given consent

B. Where state law permits such interception

C. If an organization intercepts an employee's purely personal call

D. Only if all parties have given consent

Answer: (SHOW ANSWER)

https://wyattfirm.com/the-electronic-communications-privacy-act-of-1986-tracking-the-productivity-of-work-from-home-employees/ "In other words, monitoring must be relevant to the business, recurring, and the employee must know about it." Here it is personal and there is no indication that the employee knew.

NEW QUESTION: 116

Regarding data information management, which of the following tasks can help with compliance audits, quickly comply with legal discovery requests, and ensure data is stored efficiently?

A. Data Mapping

B. Data Classification

C. Data Flow Documentation

D. Data Protection Laws

Answer: B (LEAVE A REPLY)

In general, sensitive data must have a higher classification level and should be better protected.

The number of employees who have access is then limited based on the classification level. Data classification is often mandatory in the US based on sectoral legislation. It also has advantages: it helps to comply with compliance audits, helps to quickly comply with legal (discovery) requests and storage capacity is used efficiently.

NEW QUESTION: 117

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 (LEAVE A REPLY)

The annual privacy notice requirement under the Gramm-Leach-Bliley Act (GLBA) applies to financial institutions that collect nonpublic personal information from customers and disclose it to nonaffiliated third parties, unless they qualify for an exception. A financial institution is any entity that engages in activities that are financial in nature or incidental to such activities, as defined by section 4(k) of the Bank Holding Company Act of 1956. The

King County Savings and Loan is a financial institution under this definition, as it engages in lending money and accepting deposits. Therefore, it is required to provide its customers with an annual privacy notice, unless it meets the conditions for an exception. The Four Winds Tribal College, the Golden Gavel Auction House, and the Breezy City Housing Commission are not financial institutions under the GLBA, as they do not engage in activities that are financial in nature or incidental to such activities. Therefore, they are not required to provide their customers with an annual privacy notice under the GLBA.
References:
* Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act, section I.
Background, paragraph 2.
* 17 CFR § 248.5 - Annual privacy notice to customers required., paragraph (a) (1).
* IAPP CIPP/US Study Guide, page 65.

NEW QUESTION: 118
In 2014, Google was alleged to have violated the Family Educational Rights and Privacy Act (FERPA) through its Apps for Education suite of tools. For what specific practice did students sue the company?
A. Making student education records publicly available
B. Disclosing education records without obtaining required consent
C. Scanning emails sent to and received by students
D. Relying on verbal consent for a disclosure of education records
Answer: C (LEAVE A REPLY)

NEW QUESTION: 119
Under state breach notification laws, which is NOT typically included in the definition of personal information?
A. State identification number
B. First and last name
C. Social Security number
D. Medical Information
Answer: B (LEAVE A REPLY)
Under state breach notification laws, personal information is typically defined as an individual's first name or first initial and last name plus one or more other data elements, such as Social Security number, state identification number, account number, medical information, etc. However, first and last name alone are not usually considered personal information, unless they are combined with other data elements that could identify the individual or compromise their security or privacy. Therefore, option B is the correct answer, as it is not typically included in the definition of personal information under state breach notification laws. References: https://www.ncsl.org/technology-and-communication/security-breach-notification-laws

https://iapp.org/resources/article/state-data-breach-notification-chart/

NEW QUESTION: 120
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: (SHOW ANSWER)
The U.S. Department of Commerce (DOC) is a federal agency that promotes economic growth, trade, and innovation, but does not have regulatory authority related to privacy. The DOC administers several voluntary privacy frameworks, such as the Privacy Shield, the APEC Cross- Border Privacy Rules, and the NIST Privacy Framework, but these are not legally binding or enforceable by the DOC. The DOC also participates in international privacy negotiations and dialogues, but does not have the power to issue rules or regulations on privacy matters.

NEW QUESTION: 121
What was the original purpose of the Federal Trade Commission Act?
A. To ensure privacy rights of U.S. citizens
B. To protect consumers
C. To enforce antitrust laws
D. To negotiate consent decrees with companies violating personal privacy
Answer: (SHOW ANSWER)
The Federal Trade Commission Act (FTCA) was adopted in 1914 as part of the Progressive Era reforms that aimed to curb the power and influence of monopolies and trusts in the U.S. economy. The FTCA created the Federal Trade Commission (FTC) as an independent agency to investigate and prevent unfairmethods of competition and unfair or deceptive acts or practices in or affecting commerce. The FTCA also gave the FTC the authority to issue cease and desist orders, seek injunctions, and impose civil penalties for violations of the law. The FTCA was intended to complement and supplement the existing antitrust laws, such as the Sherman Act and the Clayton Act, that prohibited restraints of trade, price-fixing, mergers, and other anticompetitive conduct.
The other options are not correct, because:
* The FTCA did not explicitly address privacy rights of U.S. citizens, although the FTC later used its authority under the FTCA to enforce against unfair or deceptive privacy practices, such as making false or misleading claims, failing to disclose material information, or violating consumers' choices or expectations regarding their personal data.
* The FTCA did not specifically focus on consumer protection, although the FTC later expanded its scope to include consumer protection issues, such as advertising and

marketing, credit and finance, privacy and security, and consumer education. The FTC also enforced other consumer protection laws, such as the Truth in Lending Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act, and the CAN-SPAM Act.
* The FTCA did not authorize the FTC to negotiate consent decrees with companies violating personal privacy, although the FTC later used consent decrees as a common tool to settle privacy cases and impose remedial measures, such as audits, reports, and compliance programs. Consent decrees are agreements between the FTC and the parties involved in a case that resolve the FTC's charges without admitting liability or wrongdoing.
References:
* FTC website, Federal Trade Commission Act
* Britannica website, Federal Trade Commission Act (FTCA)
* IAPP CIPP/US Study Guide, Chapter 1: Introduction to the U.S. Privacy Environment, pp. 11-12
* IAPP website, Federal Trade Commission Act, Section 5 of

NEW QUESTION: 122
Which of the following would NOT fall under the jurisdiction of the GDPR?
A. A German company with assets in France and employees in both companies.
B. An Italian company selling products and services worldwide.
C. A Spanish company that processes data of US citizens.
D. A US company who sells products and services in South America.
Answer: (SHOW ANSWER)
The GPDR applies to companies with assets and employees in the EU, to companies that sell to people in the EU and to data processed in the EU.

NEW QUESTION: 123
Although an employer may have a strong incentive or legal obligation to monitor employees' conduct or behavior, some excessive monitoring may be considered an intrusion on employees' privacy? Which of the following is the strongest example of excessive monitoring by the employer?

A. An employer who installs a video monitor in physical locations, such as a warehouse, to ensure employees are performing tasks in a safe manner and environment.
B. An employer who installs data loss prevention software on all employee computers to limit transmission of confidential company information.
C. An employer who installs video monitors in physical locations, such as a changing room, to reduce the risk of sexual harassment.
D. An employer who records all employee phone calls that involve financial transactions with customers completed over the phone.
Answer: C (LEAVE A REPLY)
The strongest example of excessive monitoring by the employer is C. An employer who installs video monitors in physical locations, such as a changing room, to reduce the risk of sexual harassment. This would be considered an unreasonable invasion of employees' privacy, as it would violate their legitimate expectation of privacy in a place where they change their clothes.
Such monitoring would also likely violate the Electronic Communications Privacy Act (ECPA), which prohibits the interception of oral communications without consent or authorization.
Moreover, such monitoring would not be justified by a legitimate business interest, as there are less intrusive ways to prevent or address sexual harassment, such as policies, training, and reporting mechanisms.

NEW QUESTION: 124
A financial services company install "bossware" software on its employees' remote computers to monitor performance. The software logs screenshots, mouse movements, and keystrokes to determine whether an employee is being productive. The software can also enable the computer webcams to record video footage.
Which of the following would best support an employee claim for an intrusion upon seclusion tort?
A. The webcam is enabled to record video any time the computer is turned on.
B. The company creates and saves a biometric template for each employee based upon keystroke dynamics.
C. The software automatically sends a notification to a supervisor any time the employee's mouse is dormant for more than five minutes.
D. The webcam records video of an employee using a company laptop to perform personal business while at a coffee shop during work hours.
Answer: A (LEAVE A REPLY)
An intrusion upon seclusion tort occurs when someone intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, if the intrusion would be highly offensive to a reasonable person. The intrusion does not need to involve a physical trespass, but can also be an electronic or optical intrusion, such as using

a webcam to record a person who has a reasonable expectation of privacy. The intrusion must also cause mental anguish or suffering to the plaintiff.

NEW QUESTION: 125
Which of the following data elements is most likely to be subject to comprehensive state data security and privacy laws?
A. Account holders' social security numbers, maintained by a bank.
B. Users' sexual orientations, maintained by a social media website
C. Individual drivers' license numbers, maintained by a state agency.
D. Contact details of individuals who report emergencies, maintained by local authorities
Answer: (SHOW ANSWER)
Social security numbers (SSNs) are one of the most sensitive types of personally identifiable information (PII) and are subject to comprehensive data security and privacy laws at both the federal and state levels.
Banks, as financial institutions, are subject to strict regulations under laws like the Gramm-Leach-Bliley Act (GLBA) and state privacy laws regarding the safeguarding of sensitive data like SSNs.
Why Social Security Numbers are Most Likely to Be Covered:
* SSNs are a high-value target for identity theft, making their protection a focus of numerous privacy and data security laws.
* Federal laws like GLBA and the Fair Credit Reporting Act (FCRA) impose strict data security requirements on financial institutions.
* State laws, such as those in California, often require businesses to protect SSNs and notify individuals in the event of a breach involving sensitive information.
Explanation of Options:
* A. Account holders' social security numbers, maintained by a bank:This is correct because SSNs are consistently protected under comprehensive laws at both the federal and state levels.
* B. Users' sexual orientations, maintained by a social media website:While sexual orientation may be considered sensitive data under certain laws (e.g., GDPR in the EU), U.S. privacy laws do not consistently regulate this information.
* C. Individual drivers' license numbers, maintained by a state agency:While some states regulate drivers' license data, this information is not comprehensively covered under state privacy laws.
* D. Contact details of individuals who report emergencies, maintained by local authorities:This information is regulated in limited circumstances (e.g., Freedom of Information Act or public records laws) but is not subject to comprehensive state privacy laws.
References from CIPP/US Materials:
* GLBA and FCRA: Highlight the importance of safeguarding sensitive financial information such as SSNs.

* State Data Breach Notification Laws: Many states explicitly list SSNs as a protected data element.

NEW QUESTION: 126
SCENARIO
Please use the following to answer the next QUESTION:
Cheryl is the sole owner of Fitness Coach, Inc., a medium-sized company that helps individuals realize their physical fitness goals through classes, individual instruction, and access to an extensive indoor gym. She has owned the company for ten years and has always been concerned about protecting customer's privacy while maintaining the highest level of service. She is proud that she has built long-lasting customer relationships.
Although Cheryl and her staff have tried to make privacy protection a priority, the company has no formal privacy policy. So Cheryl hired Janice, a privacy professional, to help her develop one.
After an initial assessment, Janice created a first of a new policy. Cheryl read through the draft and was concerned about the many changes the policy would bring throughout the company. For example, the draft policy stipulates that a customer's personal information can only be held for one year after paying for a service such as a session with personal trainer. It also promises that customer information will not be shared with third parties without the written consent of the customer. The wording of these rules worry Cheryl since stored personal information often helps her company to serve her customers, even if there are long pauses between their visits. In addition, there are some third parties that provide crucial services, such as aerobics instructors who teach classes on a contract basis. Having access to customer files and understanding the fitness levels of their students helps instructors to organize their classes.
Janice understood Cheryl's concerns and was already formulating some ideas for revision. She tried to put Cheryl at ease by pointing out that customer data can still be kept, but that it should be classified according to levels of sensitivity. However, Cheryl was skeptical. It seemed that classifying data and treating each type differently would cause undue difficulties in the company's day-to-day operations. Cheryl wants one simple data storage and access system that any employee can access if needed.
Even though the privacy policy was only a draft, she was beginning to see that changes within her company were going to be necessary. She told Janice that she would be more comfortable with implementing the new policy gradually over a period of several months,one department at a time. She was also interested in a layered approach by creating documents listing applicable parts of the new policy for each department.
Based on the scenario, which of the following would have helped Janice to better meet the company's needs?
A. Creating a more comprehensive plan for implementing a new policy
B. Spending more time understanding the company's information goals
C. Explaining the importance of transparency in implementing a new policy

D. Removing the financial burden of the company's employee training program

Answer: (SHOW ANSWER)

According to the Wiley study guide, one of the steps in developing a privacy policy is to conduct a privacy assessment, which involves identifying the organization's information goals and needs, as well as the legal and regulatory requirements that apply to its data collection and use practices3. By spending more time understanding the company's information goals, Janice would have been able to tailor the privacy policy to fit the company's business model and customer expectations, while still complying with the relevant privacy laws and standards. This would have also helped Janice to address Cheryl's concerns about the impact of the policy on the company's operations and customer relationships, and to propose solutions that balance privacy protection and service delivery.

References:

1: https://iapp.org/certify/cippus/

2: https://iapp.org/certify/get-certified/cippus/

3: https://www.wiley.com/en-be/IAPP+CIPP+US+Certified+Information+Privacy+Professional+Study+Guide-p-9

4: https://www.techtarget.com/searchsecurity/quiz/10-CIPP-US-practice-questions-to-test-your-privacy-knowledge

5: https://www.study4exam.com/iapp/free-cipp-us-questions

https://www.passitcertify.com/iapp/cipp-us-questions.html

NEW QUESTION: 127

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

pnvacy 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.
Which of the following would accurately describe the relationship of the parties if they enter into a contract for use of the app?
A. Miraculous Healthcare would be the covered entity because Us name and branding are on the app. MedApps would be a business associate because it Is hosting the data that supports the app
B. MedApps would be the covered entity because it built and hosts the app and all the data.
Miraculous Healthcare would be a business associate because it only provides its brand on the app.
C. Miraculous Healthcare would be a covered entity because it is the healthcare provider; MedApps would also be a covered entity because the data in the app is being shared with it.
D. Miraculous Healthcare would be the covered entity because it is the healthcare provider; MedApps would be a business associate because it is providing a service to support Miraculous.
Answer: D (LEAVE A REPLY)
Under the Health Insurance Portability and Accountability Act (HIPAA), entities involved in the handling of protected health information (PHI) are classified as either covered entities or business associates based on their roles and activities.
Definitions Under HIPAA:
Covered Entity (CE):
A healthcare provider, health plan, or healthcare clearinghouse that creates, receives, maintains, or transmits PHI.
Miraculous Healthcare qualifies as a covered entity because it is a medical practice directly providing healthcare services to patients.
Business Associate (BA):
An organization or individual that performs functions, activities, or services involving the use or disclosure of PHI on behalf of a covered entity.
MedApps qualifies as a business associate because it is providing a telehealth app service to Miraculous, which involves hosting and maintaining PHI (e.g., appointment details, patient information).
Analysis of the Relationship:
Miraculous Healthcare: As the healthcare provider, it is responsible for patient care and compliance with HIPAA. Since it directly provides healthcare services to patients, it is the covered entity in this scenario.
MedApps: Although MedApps designed, hosts, and supports the telehealth app, it is providing these services on behalf of Miraculous Healthcare. As such, MedApps is a

business associate under HIPAA. This designation requires MedApps to comply with HIPAA regulations through a Business Associate Agreement (BAA), ensuring that it appropriately safeguards the PHI it handles on behalf of Miraculous Healthcare.
Consideration of the Benchmarking Service:

NEW QUESTION: 128
What privacy concept grants a consumer the right to view and correct errors on his or her credit report?
A. Action.
B. Access.
C. Notice.
D. Choice.
Answer: (SHOW ANSWER)

NEW QUESTION: 129
More than half of U.S. states require telemarketers to?
A. Identify themselves at the beginning of a call
B. Obtain written consent from potential customers
C. Register with the state before conducting business
D. Provide written contracts for customer transactions
Answer: (SHOW ANSWER)
According to the IAPP CIPP/US Study Guide, more than half of U.S. states require telemarketers to register with the state before conducting business within the state. This registration requirement may involve paying a fee, posting a bond, or providing information about the telemarketer's identity, location, and business practices. The purpose of this requirement is to protect consumers from fraudulent or deceptive telemarketing calls and to facilitate the enforcement of state laws and regulations.

NEW QUESTION: 130
What is a legal document approved by a judge that formalizes an agreement between a governmental agency and an adverse party called?
A. A consent decree
B. Stare decisis decree
C. A judgment rider
D. Common law judgment
Answer: (SHOW ANSWER)
A consent decree is a legal document that resolves a dispute between a governmental agency and an adverse party without admission of guilt or liability by either side. It is approved by a judge and has the force of a court order. A consent decree may include terms such as compliance, monitoring, reporting, or remediation. A consent decree is often used to settle civil enforcement actions brought by federal agencies such as the Federal

Trade Commission (FTC), the Environmental Protection Agency (EPA), or the Department of Justice (DOJ).

NEW QUESTION: 131
Which of the following types of information would an organization generally NOT be required to disclose to law enforcement?
A. Information about medication errors under the Food, Drug and Cosmetic Act
B. Money laundering information under the Bank Secrecy Act of 1970
C. Information about workspace injuries under OSHA requirements
D. Personal health information under the HIPAA Privacy Rule
Answer: D (LEAVE A REPLY)
These are "permissive" disclosures. The covered entity or business associate may refuse. https://www.eff.org/issues/law-enforcement-

NEW QUESTION: 132
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. Bill the majority of patients electronically for their health care
B. Keep electronic updates about the Health Insurance Portability and Accountability Act
C. Make electronic health records (EHRs) part of regular care
D. Send health information and appointment reminders to patients electronically
Answer: C (LEAVE A REPLY)

NEW QUESTION: 133
Which of the following became the first state to pass a law specifically regulating the practices of data brokers?
A. Washington.
B. California.
C. New York.
D. Vermont.
Answer: D (LEAVE A REPLY)
According to the web search results from my predefined tool, Vermont became the first state to pass a law specifically regulating the practices of data brokers in 2018. The law defines a data broker as "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." The law requires data brokers to register with the Secretary of State, pay a registration fee, provide information about their data collection and opt-out practices, and implement security measures to protect the personal information they collect and sell. The law also imposes additional obligations on data brokers that possess the personal information of

minors. The law aims to increase the transparency and accountability of the data broker industry and to protect the privacy rights of consumers12. References:
* Registered Data Brokers in the United States: 2021 | Privacy Rights ...
* Am I A Data Broker?: A Quick Primer on State Laws Regulating a ... - Taft

NEW QUESTION: 134
Under GLBA. which of these organizations would not be required to provide its customers with an annual privacy notice?
A. An insurance company that has no privacy department
B. An auction house that also acts as a financial institution
C. A credit union that has made changes to its privacy notice from last year.
D. A credit union that has not made changes to its privacy notice from last year
Answer: D (LEAVE A REPLY)
Under the Gramm-Leach-Bliley Act (GLBA), financial institutions are required to provide their customers with an annual privacy notice that explains how they collect, share, and protect customers' personal information. However, the GLBA Privacy Rule (16 CFR Part 313) was amended by the Fixing America's Surface Transportation Act (FAST Act) in 2015, which introduced an exception to this requirement.
According to the FAST Act, financial institutions are not required to provide annual privacy notices if they meet two conditions:
No changes have been made to their privacy policy or practices since the last notice was sent to customers.
The financial institution does not share customers' nonpublic personal information with nonaffiliated third parties in a way that triggers an opt-out requirement under GLBA.

NEW QUESTION: 135
A company based in United States receives information about its UK subsidiary's employees in connection with the centralized HR service it provides.
How can the UK company ensure an adequate level of data protection that would allow the restricted data transfer to continue?
A. By signing up to an approved code of conduct under UK GDPR to demonstrate compliance with its requirements, both for the parent and the subsidiary companies.
B. By revising the contract with the United States parent company incorporating EU SCCs, as it continues to be valid for restricted transfers under the UK regime.
C. By submitting to the ICO a new application for the UK BCRs using the UK BCR application forms, as their existing authorized EU BCRs are not recognized.
D. By allowing each employee the option to opt-out to the restricted transfer, as it is necessary to send their names in order to book the sales bonuses.
Answer: (SHOW ANSWER)
The UK company can ensure an adequate level of data protection for the restricted data transfer to the US parent company by using the EU Standard Contractual Clauses (SCCs),

which are contractual terms that provide safeguards for personal data transferred from the UK to third countries. The UK GDPR recognizes the validity of the EU SCCs adopted before the end of the Brexit transition period, and allows the UK Information Commissioner's Office (ICO) to issue new SCCs in the future. The other options are not correct because:

* A. Signing up to an approved code of conduct under the UK GDPR is not sufficient to ensure an adequate level of data protection for restricted transfers, as it is not a transfer mechanism on its own.

The UK company would still need to use another appropriate safeguard, such as SCCs or Binding Corporate Rules (BCRs), to transfer personal data to the US parent company.

* C. Submitting a new application for the UK BCRs is not necessary, as the UK GDPR recognizes the existing authorized EU BCRs as valid for restricted transfers from the UK. The UK company can continue to rely on its EU BCRs, as long as they are updated to reflect the UK GDPR requirements and the role of the ICO as the competent supervisory authority.
* D. Allowing each employee the option to opt-out to the restricted transfer is not a valid transfer mechanism under the UK GDPR, as it does not provide adequate safeguards for the personal data of the employees. The UK company would need to obtain the explicit consent of each employee for the restricted transfer, which must be freely given, specific, informed, and unambiguous. References:
* UK GDPR, Chapter V, Article 46
* UK GDPR, Chapter V, Article 47
* UK GDPR, Chapter V, Article 49
* ICO guidance on international transfers
* IAPP CIPP/US Study Guide, Chapter 10, Section 10.3.2

NEW QUESTION: 136

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?

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 (LEAVE A REPLY)

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,
202. 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, 202. 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, 202. 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.

NEW QUESTION: 137
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 FISA. 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: (SHOW ANSWER)
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.

NEW QUESTION: 138
SCENARIO
Please use the following to answer the next QUESTION:
You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data.
However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.
A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has

launched similar attacks on other hospitals - ones that exposed the PHI of public figures including celebrities and politicians.
During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.
A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as aresult of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.
Of the safeguards required by the HIPAA Security Rule, which of the following is NOT at issue due to HealthCo's actions?
A. Administrative Safeguards
B. Technical Safeguards
C. Physical Safeguards
D. Security Safeguards
Answer: D (LEAVE A REPLY)
The HIPAA Security Rule requires covered entities and their business associates to implement three types of safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI): administrative, physical, and technical1. Security safeguards is not a separate category of safeguards, but rather a general term that encompasses all three types. Therefore, it is not a correct answer to the question.
* Administrative safeguards are the policies and procedures that govern the conduct of the workforce and the security measures put in place to protect ePHI. They include risk analysis and management, training, contingency planning, incident response, and evaluation12.
* Physical safeguards are the locks, doors, cameras, and other physical measures that prevent unauthorized access to ePHI. They include workstation and device security, locks and keys, and disposal of media12.
* Technical safeguards are the software and hardware tools that protect ePHI from unauthorized access, alteration, or destruction. They include access control, encryption, audit controls, integrity controls, and transmission security12.
In the scenario, HealthCo's actions have potentially violated all three types of safeguards. For example:
* HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures. This could be a breach of the administrative safeguard of risk analysis and management12.
* HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. This could be a breach of the technical safeguard of encryption12.

* HealthCo provides its investigative report of the breach and a copy of the PHI of the individuals affected to law enforcement. This could be a breach of the physical safeguard of disposal of media, if HealthCo did not ensure that the media was properly erased or destroyed after the transfer12.
References: 1: Summary of the HIPAA Security Rule, HHS.gov. 2: What is the HIPAA Security Rule?
Safeguards ... - Secureframe, Secureframe.com.

NEW QUESTION: 139
What was the original purpose of the Federal Trade Commission Act?
A. To ensure privacy rights of U.S. citizens
B. To protect consumers
C. To enforce antitrust laws
D. To negotiate consent decrees with companies violating personal privacy
Answer: C (LEAVE A REPLY)
IAPP book, Section 3.3, first sentence. "The FTC was founded in 1914 to enforce antitrust laws, and its general consumer protection mission was established by a statutory change in 1938." In particular in considering this answer, note that the FTC Act was initially passed in 1914.

NEW QUESTION: 140
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 (LEAVE A REPLY)
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.
References:
* IAPP CIPP/US Body of Knowledge, Domain II: Limits on Private-sector Collection and Use of Data, Section B: Communications and Marketing
* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 2: Limits on Private-sector Collection and Use of Data, Section 2.2: Communications and Marketing

* Practice Exam - International Association of Privacy Professionals

NEW QUESTION: 141
California's SB 1386 was the first law of its type in the United States to do what?
A. Require commercial entities to disclose a security data breach concerning personal information about the state's residents
B. Require notification of non-California residents of a breach that occurred in California
C. Require encryption of sensitive information stored on servers that are Internet connected
D. Require state attorney general enforcement of federal regulations against unfair and deceptive trade practices
Answer: A (LEAVE A REPLY)
California's SB 1386, also known as the California Security Breach Information Act, was enacted in 2002 and became effective in 2003. It was the first law of its kind in the United States to require commercial entities that own or license personal information of California residents to notify them in the event of a security breach that compromises their unencrypted data. The law aims to protect the privacy and security of personal information and to enable individuals to take preventive measures against identity theft and fraud. The law applies to any business or person that conducts business in California and that owns or licenses computerized data that includes personal information, as defined by the law. Personal information includes an individual's first name or first initial and last name in combination with any one or more of the following data elements: Social Security number, driver's license number or California identification card number, account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, or medical information or health insurance information. The law does not apply to encrypted information, publicly available information, or information that is lawfully obtained from federal, state, or local government records. The law requires the disclosure of a breach of the security of the system to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The disclosure may be made by written notice, electronic notice, or substitute notice, as specified by the law. The law also requires any person or business that maintains computerized data that includes personal information that the person or business does not own to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The law also authorizes a civil action for damages by a customer injured by a violation of the law and provides that the rights and remedies available under the law are

cumulative to each other and to any other rights and remedies available under law.
References:
* California Senate Bill 1386 (2002)
* California SB 1386: For the Love of Privacy
* What Is the California Security Breach Information Act?
* California Raises the Bar on Data Security and Privacy

NEW QUESTION: 142
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 (LEAVE A REPLY)
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. References:
* HIPAA Rules for Medical Billing - Compliancy Group
* HIPAA Compliance for Billing Companies: Easy Guide - iFax

NEW QUESTION: 143
Which federal agency plays a role in privacy policy, but does NOT have regulatory authority?
A. The Office of the Comptroller of the Currency.
B. The Federal Communications Commission.
C. The Department of Transportation.
D. The Department of Commerce.
Answer: D (LEAVE A REPLY)
Per page 35 of the book, the DOC does not have regulatory authority for privacy. The FTC is separate from that of the DOC. FTC is a independent agency and the DOC is a department within the executive branch.

NEW QUESTION: 144
When designing contact tracing apps in relation to COVID-19 or any other diagnosed virus, all of the following privacy measures should be considered EXCEPT?
A. Data retention.
B. Use limitations.
C. Opt-out choice.
D. User confidentiality.
Answer: C (LEAVE A REPLY)
Contact tracing apps are designed to help public health authorities track and contain the spread of COVID-19 or any other diagnosed virus by notifying users who have been in close contact with an infected person. However, these apps also raise privacy concerns, as they collect and process sensitive personal data, such as health status and location information. Therefore, contact tracing apps should follow the principles of privacy by design and default, which means that they should incorporate privacy measures into their development and operation, and offer the highest level of privacy protection to users.
Some of the privacy measures that should be considered when designing contact tracing apps are:
Data retention: Contact tracing apps should only retain the personal data they collect for as long as necessary to achieve their public health purpose, and delete or anonymize the data afterwards. Data retention periods should be clearly communicated to users and based on scientific evidence and legal requirements.
Use limitations: Contact tracing apps should only use the personal data they collect for the specific and legitimate purpose of contact tracing, and not for any other purposes, such as commercial, law enforcement, or surveillance. Use limitations should be enforced by technical and organizational measures, such as encryption, access controls, and audits.
User confidentiality: Contact tracing apps should protect the confidentiality of users' personal data and identity, and not disclose them to third parties without their consent or legal authorization. User confidentiality should be ensured by technical and organizational measures, such as pseudonymization, aggregation, and data minimization.
Opt-out choice, on the other hand, is not a privacy measure that should be considered when designing contact tracing apps, as it would undermine their effectiveness and public health objective. Contact tracing apps rely on voluntary participation and widespread adoption by users to function properly and achieve their purpose. Therefore, offering users the option to opt out of the app or certain features, such as data sharing or notifications, would reduce the app's coverage and accuracy, and potentially expose users and others to greater health risks. Instead of opt-out choice, contact tracing apps should provide users with clear and transparent information about how the app works, what data it collects and how it uses it, what benefits and risks it entails, and what rights and controls users have over their data. This way, users can make an informed and voluntary decision to use the app or not, based on their own preferences and values.

NEW QUESTION: 145
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: (SHOW ANSWER)
The Red Flag Program Clarification Act of 2010 amended the original Red Flags rule, which required certain financial institutions and creditors to develop and implement a written identity theft prevention program. The Clarification Act narrowed the definition of creditor to include only those who regularly and in the ordinary course of business advance funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person12. This excludes creditors who advance funds for expenses incidental to a service provided by the creditor to that person3. References:
* CIPP/US Practice Questions (Sample Questions), Question 133, Answer B, Explanation B.
* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4, Section 4.3, p. 108-
109.
* Red Flag Program Clarification Act of 2010, Section 2, Subsection (b).

NEW QUESTION: 146
Which of the following best describes an employer's privacy-related responsibilities to an employee who has left the workplace?
A. An employer has a responsibility to maintain a former employee's access to computer systems and company data needed to support claims against the company such as discrimination.
B. An employer has a responsibility to permanently delete or expunge all sensitive employment records to minimize privacy risks to both the employer and former employee.
C. An employer may consider any privacy-related responsibilities terminated, as the relationship between employer and employee is considered primarily contractual.
D. An employer has a responsibility to maintain the security and privacy of any sensitive employment records retained for a legitimate business purpose.
Answer: D (LEAVE A REPLY)
Employers have a duty to protect the personal information of their current and former employees, as well as applicants, from unauthorized access, use, or disclosure. This duty may arise from federal or state laws, such as the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), or the California Consumer Privacy Act (CCPA), or from contractual obligations, such as non-disclosure agreements or

privacy policies. Employers may retain sensitive employment records, such as performance evaluations, disciplinary actions, medical records, or background checks, for a legitimate business purpose, such as complying with legal requirements, defending against lawsuits, or conducting audits. However, employers must ensure that these records are stored securely, accessed only by authorized personnel, and disposed of properly when no longer needed. References: IAPP CIPP/US Study Guide, Chapter 4, Section
4.1.1, IAPP CIPP/US Body of Knowledge, Domain IV, Objective B

NEW QUESTION: 147
What is the purpose of a cure provision in a stale data privacy law?
A. To allow a business a limited timeframe to fix alleged violations before facing enforcement.
B. To allow consumers a period of time to discover their data has been mishandled
C. To allow a state to initiate formal enforcement actions for a fixed time period.
D. To allow certain provisions of a law to expire after a defined time period
Answer: A (LEAVE A REPLY)
A cure provision in state data privacy laws gives businesses an opportunity to remediate violations of the law within a specified timeframe after receiving notice of the alleged violation.
This provision is intended to promote compliance rather than immediately imposing penalties or enforcement actions.
Key Aspects of Cure Provisions:
Notice and Cure Period:
Businesses are given a timeframe (e.g., 30 days) to address the alleged violation before formal enforcement actions are taken by state authorities.
Encouraging Compliance:
Cure provisions incentivize businesses to implement corrective actions and ensure compliance without incurring fines or penalties for minor or first-time violations.
State-Specific Examples:
The California Consumer Privacy Act (CCPA) initially included a 30-day cure provision, though it was later limited under the California Privacy Rights Act (CPRA). Other state laws, such as Virginia's Consumer Data Protection Act (VCDPA), also include cure provisions.

NEW QUESTION: 148
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 Station's network and was able to steal data relating to employees in the company'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.
The Board has asked Otto whether the company will need to comply with the new California Consumer Privacy Law (CCPA). What should Otto tell the Board?
A. That CCPA will apply to the company only after the California Attorney General determines that it will enforce the statute.
B. That the company is governed by CCPA, but does not need to take any additional steps because it follows CPBR.
C. That business contact information could be considered personal information governed by CCPA.
D. That CCPA only applies to companies based in California, which exempts the company from compliance.
Answer: C (LEAVE A REPLY)
The CCPA applies to any business that collects personal information of California residents, regardless of where the business is located1. The CCPA defines personal information broadly as any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household2. This could include business contact information, such as name, email address, phone number, or job title, if it is linked to a specific individual3. Therefore, Otto should tell the Board that business contact information could be considered personal information governed by CCPA, and that the company may need to comply with the CCPA requirements, such as providing notice, honoring consumer rights requests, and implementing reasonable security measures4. References:
* CIPP/US Practice Questions (Sample Questions), Question 124, Answer C, Explanation C.

* IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 6, Section 6.2, p.
181-182.
* California Consumer Privacy Act (CCPA), Section 1798.140, Subsection (o).
* CCPA Compliance Checklist for Businesses, Section 2, Subsection (a).

NEW QUESTION: 149
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 (LEAVE A REPLY)
Some types of businesses are not covered by the TSR even though they conduct telemarketing campaigns that may involve some interstate telephone calls to sell goods or services. These three types of entities are not subject to the FTC's jurisdiction, and are not covered by the TSR:
1. banks, federal credit unions, and federal savings and loans.
2. common carriers - such as long-distance telephone companies and airlines - when they are engaging in common carrier activity.
3. NON-PROFIT ORGANIZATIONS - those entities that are not organized to carry on business for their own, or their members', profit.
https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#comply

NEW QUESTION: 150
Which of the following best describes the ASIA-Pacific Economic Cooperation (APEC) principles?
A. A bill of rights for individuals seeking access to their personal information.
B. A code of responsibilities for medical establishments to uphold privacy laws.
C. An international court ruling on personal information held in the commercial sector.
D. A baseline of marketers' minimum responsibilities for providing opt-out mechanisms.
Answer: (SHOW ANSWER)
The APEC principles are part of the APEC Privacy Framework, which is an inter-governmental agreement among the 21 member economies of the Asia-Pacific Economic Cooperation (APEC) to promote information privacy protection and the free flow of information in the region. The APEC Privacy Framework consists of four parts: a preamble, a scope, a set of nine information privacy principles, and an implementation section. The APEC information privacy principles are:

Preventing harm: Personal information controllers should take reasonable steps to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction, and to address the risks and challenges posed by specific technologies and business practices. Notice: Personal information controllers should provide clear and easily accessible statements about their personal information handling practices, including the types of personal information they collect, the purposes for which they collect it, the types of third parties to which they disclose it, the choices and means they offer individuals for limiting the use and disclosure of their personal information, and how they can contact the personal information controller with inquiries or complaints.

NEW QUESTION: 151
What do the Civil Rights Act, Pregnancy Discrimination Act, Americans with Disabilities Act, Age Discrimination Act, and Equal Pay Act all have in common?
A. They require employers not to discriminate against certain classes when employees use personal information
B. They require that employers provide reasonable accommodations to certain classes of employees
C. They afford certain classes of employees' privacy protection by limiting inquiries concerning their personal information
D. They permit employers to use or disclose personal information specifically about employees who are members of certain classes
Answer: (SHOW ANSWER)
The Civil Rights Act, Pregnancy Discrimination Act, Americans with Disabilities Act, Age Discrimination Act, and Equal Pay Act are all federal laws that prohibit employment discrimination based on certain protected characteristics, such as race, sex, disability, age, and pay. These laws also afford certain classes of employees' privacy protection by limiting inquiries concerning their personal information that may reveal their protected status or be used for discriminatory purposes.

NEW QUESTION: 152
Under GLBA. which of these organizations would not be required to provide its customers with an annual privacy notice?

A. An insurance company that has no privacy department
B. An auction house that also acts as a financial institution
C. A credit union that has made changes to its privacy notice from last year.
D. A credit union that has not made changes to its privacy notice from last year
Answer: D (LEAVE A REPLY)
Under the Gramm-Leach-Bliley Act (GLBA), financial institutions are required to provide their customers with an annual privacy notice that explains how they collect, share, and protect customers' personal information. However, the GLBA Privacy Rule (16 CFR Part 313) was amended by the Fixing America's Surface Transportation Act (FAST Act) in 2015, which introduced an exception to this requirement.
According to the FAST Act, financial institutions are not required to provide annual privacy notices if they meet two conditions:
* No changes have been made to their privacy policy or practices since the last notice was sent to customers.
* The financial institution does not share customers' nonpublic personal information with nonaffiliated third parties in a way that triggers an opt-out requirement under GLBA.
Explanation of Options:
* A. An insurance company that has no privacy department: This is irrelevant. The requirement to provide privacy notices depends on whether the organization falls under GLBA's definition of a
"financial institution" and their compliance with privacy practices, not on the presence of a privacy department.
* B. An auction house that also acts as a financial institution: If the auction house qualifies as a financial institution under GLBA (e.g., if it arranges financing), it would still need to comply with GLBA privacy requirements, including issuing annual privacy notices unless it qualifies for the exception.
* C. A credit union that has made changes to its privacy notice from last year: If any changes are made to the privacy policy, the credit union must issue an updated privacy notice to its customers.
* D. A credit union that has not made changes to its privacy notice from last year: This is the correct answer. If the credit union has not made any changes to its privacy notice and meets the FAST Act exception criteria (outlined above), it is not required to issue an annual privacy notice.
References from CIPP/US Materials:
* GLBA Privacy Rule (16 CFR Part 313): This rule outlines the requirements for financial institutions to provide privacy notices.
* FAST Act (2015) Amendment to GLBA Privacy Rule: This amendment introduced exceptions to the annual notice requirement for institutions that meet specific criteria.
* IAPP CIPP/US Certification Textbook: Details the conditions under which GLBA exceptions apply and describes how the FAST Act impacted annual privacy notice requirements.

NEW QUESTION: 153
Which of the following best describes how federal anti-discrimination laws protect the privacy of private-sector employees in the United States?
A. They limit the types of information that employers can collect about employees.
B. They limit the amount of time a potential employee can be interviewed.
C. They prescribe working environments that are safe and comfortable.
D. They promote a workforce of employees with diverse skills and interests.
Answer: (SHOW ANSWER)

NEW QUESTION: 154
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: (SHOW ANSWER)

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.1 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.2 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.3 References: 1: Complying with COPPA: Frequently Asked Questions4, Section A2: COPPA Safe Harbor Program3: IAPP CIPP/US Certified Information Privacy Professional Study Guide, page 143.

NEW QUESTION: 155

SCENARIO

Please use the following to answer the next QUESTION:

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

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

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

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

What is the most significant reason that the U.S. Department of Health and Human Services (HHS) might impose a penalty on HealthCo?

A. Because HealthCo did not require CloudHealth to implement appropriate physical and administrative measures to safeguard the ePHI

B. Because HealthCo did not conduct due diligence to verify or monitor CloudHealth's security measures

C. Because HIPAA requires the imposition of a fine if a data breach of this magnitude has occurred

D. Because CloudHealth violated its contract with HealthCo by not encrypting the ePHI

Answer: (SHOW ANSWER)

According to the HIPAA Security Rule, covered entities are responsible for ensuring that their business associates comply with the security standards and safeguards required by the rule. This includes conducting due diligence to assess the business associate's security capabilities and practices, and monitoring their performance and compliance. Failure to do so may result in a violation of the rule and a penalty by the HHS.

In this scenario, HealthCo did not perform due diligence on CloudHealth before entering the contract, and did not conduct audits of CloudHealth's security measures. This is the most significant reason why HHS might impose a penalty on HealthCo, as it indicates a lack of oversight and accountability for the protection of ePHI. References:

* HIPAA Security Rule
* HIPAA Business Associate Contracts
* HIPAA Enforcement and Penalties

NEW QUESTION: 156

SCENARIO

Please use the following to answer the next QUESTION

Felicia has spent much of her adult life overseas, and has just recently returned to the U.S. to help her friend Celeste open a jewelry store in California. Felicia, despite being excited at the prospect, has a number of security concerns, and has only grudgingly accepted the need to hire other employees. In order to guard against the loss of valuable merchandise, Felicia wants to carefully screen applicants. With their permission, Felicia would like to run credit checks, administer polygraph tests, and scrutinize videos of interviews. She intends to read applicants' postings on social media, ask questions about drug addiction, and solicit character references. Felicia believes that if potential employees are serious about becoming part of a dynamic new business, they will readily agree to these requirements.
Felicia is also in favor of strict employee oversight. In addition to protecting the inventory, she wants to prevent mistakes during transactions, which will require video monitoring. She also wants to regularly check the company vehicle's GPS for locations visited by employees. She also believes that employees who use their own devices for work-related purposes should agree to a certain amount of supervision.
Given her high standards, Felicia is skeptical about the proposed location of the store. She has been told that many types of background checks are not allowed under California law. Her friend Celeste thinks these worries are unfounded, as long as applicants verbally agree to the checks and are offered access to the results.
Nor does Celeste share Felicia's concern about state breach notification laws, which, she claims, would be costly to implement even on a minor scale. Celeste believes that even if the business grows a customer database of a few thousand, it's unlikely that a state agency would hassle an honest business if an accidental security incident were to occur. In any case, Celeste feels that all they need is common sense - like remembering to tear up sensitive documents before throwing them in the recycling bin. Felicia hopes that she's right, and that all of her concerns will be put to rest next month when their new business consultant (who is also a privacy professional) arrives from North Carolina.
Which law will be most relevant to Felicia's plan to ask applicants about drug addiction?
A. The Americans with Disabilities Act (ADA).
B. The Occupational Safety and Health Act (OSHA).
C. The Genetic Information Nondiscrimination Act of 2008.
D. The Health Insurance Portability and Accountability Act (HIPAA).
Answer: (SHOW ANSWER)
The ADA prohibits employers from discriminating against qualified individuals with disabilities in all aspects of employment, including hiring, firing, promotion, compensation, and training. The ADA also limits the types of medical inquiries and examinations that employers can make of applicants and employees. Under the ADA, a disability is defined as a physical or mental impairment that substantially limits one or more major life activities, a record of such an impairment, or being regarded as having such an impairment. The ADA covers current, past, and perceived drug addiction as a disability, unless the individual is currently engaging in the illegal use of drugs. Therefore, Felicia's plan to ask applicants about drug addiction may violate the ADA, unless she can show that the inquiry

is job-related and consistent with business necessity. The other laws are not directly relevant to Felicia's plan, although they may have other implications for her business.
References: ADA, IAPP CIPP/US Study Guide (p. 95-96)

NEW QUESTION: 157
The Cable Communications Policy Act of 1984 requires which activity?
A. Delivery of an annual notice detailing how subscriber information is to be used
B. Destruction of personal information a maximum of six months after it is no longer needed
C. Notice to subscribers of any investigation involving unauthorized reception of cable services
D. Obtaining subscriber consent for disseminating any personal information necessary to render cable services
Answer: A (LEAVE A REPLY)
The Cable Communications Policy Act of 1984 (CCPA) is a federal law that regulates the cable television industry and protects the privacy of cable subscribers. One of the provisions of the CCPA is that cable operators must providetheir subscribers with an annual notice that clearly and conspicuously informs them of the following information12:
* The nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information
* The nature, frequency, and purpose of any disclosure of such information, including an identification of the types of persons to whom the disclosure may be made
* The period during which such information will be maintained by the cable operator
* The times and place at which the subscriber may have access to such information
* The limitations provided by the CCPA with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under the CCPA to enforce such limitations The annual notice must also state that the subscriber has the right to prevent disclosure of personally identifiable information to third parties, except as required by law or court order, and that the subscriber may sue for damages, attorney's fees, and other relief for violations of the CCPA12.
References: 1: Cable Communications Policy Act of 1984, Section 631 2: [IAPP CIPP/US Study Guide], Chapter 8, Section 8.3.2

NEW QUESTION: 158
SCENARIO
Please use the following to answer the next question:
You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in statea. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo.

CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.
A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals ?ones that exposed the PHI of public figures including celebrities and politicians.
During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.
A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.
What is the most effective kind of training CloudHealth could have given its employees to help prevent this type of data breach?
A. Training on techniques for identifying phishing attempts
B. Training on the terms of the contractual agreement with HealthCo
C. Training on the difference between confidential and non-public information
D. Training on CloudHealth's HR policy regarding the role of employees involved data breaches
Answer: (SHOW ANSWER)
Phishing is a form of social engineering that involves sending fraudulent emails or other messages that appear to come from a legitimate source, but are designed to trick recipients into revealing sensitive information, such as passwords, account numbers, or personal identifiers.
Phishing is one of the most common and effective methods of cyberattacks, and it can lead to data breaches, identity theft, ransomware infections, or other serious consequences. Therefore, training on how to recognize and avoid phishing attempts is crucial for any organization that handles sensitive data, especially ePHI, which is subject to strict regulations under HIPAA.

NEW QUESTION: 159
Which entities must comply with the Telemarketing Sales Rule?
A. Nonprofit organizations calling on their own behalf

B. For-profit and not-for-profit organizations when selling additional services to establish customers
C. For-profit organizations calling businesses when a binding contract exists between them
D. For-profit organizations and for-profit telefunders regarding charitable solicitations
Answer: (SHOW ANSWER)

NEW QUESTION: 160
What is the main purpose of requiring marketers to use the Wireless Domain Registry?
A. To access a current list of wireless domain names
B. To prevent unauthorized emails to mobile devices
C. To acquire authorization to send emails to mobile devices
D. To ensure their emails are sent to actual wireless subscribers
Answer: B (LEAVE A REPLY)
The Wireless Domain Registry is a list of domain names that are used to transmit electronic messages to wireless devices, such as cell phones and pagers. The purpose of the registry is to protect wireless consumers from unwanted commercial electronic mail messages, by identifying the domain names for those who send such messages. Marketers are required to use the registry to avoid sending unsolicited emails to wireless devices, which may incur costs or inconvenience for the recipients. Sending such emails without the express prior authorization of the recipient is a violation of the CAN-SPAM Act of 2003. References: https://www.
fcc.gov/cgb/policy/domain-name-input
https://www.prnewswire.com/in/news-releases/the-wireless-registry-launches-worlds-first-global- registry-for-wireless-names-240222521.html

NEW QUESTION: 161
Which of the following federal agencies does NOT enforce the Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA)?
A. The Consumer Financial Protection Bureau
B. The Office of the Comptroller of the Currency
C. The Federal Trade Commission
D. The Department of Health and Human Services
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
SuperMart is a large Nevada-based business that has recently determined it sells what constitutes "covered information" under Nevada's privacy law, Senate Bill 260. Which of the following privacy compliance steps would best help SuperMart comply with the law?
A. Providing a mechanism for consumers to opt out of sales.
B. Implementing internal protocols for handling access and deletion requests.

C. Preparing a notice of financial incentive for any loyalty programs offered to its customers.
D. Reviewing its vendor contracts to ensure that the vendors are subject to service provider restrictions.
Answer: A (LEAVE A REPLY)
SB 260 relates to consumer ability to opt-out of PII sales by data brokers.
https://www.leg.state.nv.us/App/NELIS/REL/81st2021/Bill/7805/Text

NEW QUESTION: 163
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 participating in an approved self-regulatory program
B. By regularly assessing the security risks to consumer privacy
C. By receiving FTC approval for the content of its emails
D. By making a COPPA privacy notice available on website
Answer: C (LEAVE A REPLY)

NEW QUESTION: 164

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 dat a. 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.
Under the General Data Protection Regulation (GDPR), how would the U.S.-based startup company most likely be classified?
A. As a data supervisor
B. As a data processor
C. As a data controller
D. As a data manager
Answer: B (LEAVE A REPLY)
Processor is the answer and correct based on the fact that the EU retailer was collecting consents and sending data internationally to US. The distractor of lack of consent and the instruction somehow implied that it now needs to be adhered to by the processor despite controller EU Retailer messing up should be mindfully sidestepped. Supervisor and Controller are synonymous with both terms used in the GDPR. Data manager is not a term used in GDPR.

NEW QUESTION: 165
Which of the following types of information would an organization generally NOT be required to disclose to law enforcement?
A. Information about medication errors under the Food, Drug and Cosmetic Act
B. Money laundering information under the Bank Secrecy Act of 1970
C. Information about workspace injuries under OSHA requirements
D. Personal health information under the HIPAA Privacy Rule
Answer: D (LEAVE A REPLY)

The HIPAA Privacy Rule generally prohibits covered entities and business associates from disclosing protected health information (PHI) to law enforcement without the individual's authorization, unless one of the exceptions in 45 CFR ?164.512 applies. These exceptions include disclosures required by law, disclosures for law enforcement purposes, disclosures about victims of abuse, neglect or domestic violence, disclosures for health oversight activities, disclosures for judicial and administrative proceedings, disclosures for research purposes, disclosures to avert a serious threat to health or safety, disclosures for specialized government functions, disclosures for workers' compensation, and disclosures to coroners and medical examiners. None of these exceptions apply to the type of information in option D, which is personal health information that is not related to any of the above purposes. Therefore, an organization would generally not be required to disclose such information to law enforcement under the HIPAA Privacy Rule.

NEW QUESTION: 166

SCENARIO

Please use the following to answer the next QUESTION:

Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. "If they were really serious about not being bothered," Evan said, "They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to." Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call "another time." This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.

Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social medi a. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions. Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.

Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an

undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
In regard to telemarketing practices, Evan the supervisor has a misconception regarding?
A. The right to monitor calls for quality assurance
B. The conditions under which recipients can opt out
C. The wishes of recipients who request callbacks
D. The relationship of state law to federal law
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
Which of the following is NOT one of three broad categories of products offered by data brokers, as identified by the U.S. Federal Trade Commission (FTC)?
A. Location of individuals (such as identifying an individual from partial information).
B. Research (such as information for understanding consumer trends).
C. Risk mitigation (such as information that may reduce the risk of fraud).
D. Marketing (such as appending data to customer information that a marketing company already has).
Answer: A (LEAVE A REPLY)

NEW QUESTION: 168
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 (LEAVE A REPLY)

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.

NEW QUESTION: 169
Acme Student Loan Company has developed an artificial intelligence algorithm that determines whether an individual is likely to pay their bill or default. A person who is determined by the algorithm to be more likely to default will receive frequent payment reminder calls, while those who are less likely to default will not receive payment reminders.
Which of the following most accurately reflects the privacy concerns with Acme Student Loan Company using artificial intelligence in this manner?
A. If the algorithm uses risk factors that impact the automatic decision engine. Acme must ensure that the algorithm does not have a disparate impact on protected classes in the output.
B. If the algorithm makes automated decisions based on risk factors and public information, Acme need not determine if the algorithm has a disparate impact on protected classes.
C. If the algorithm's methodology is disclosed to consumers, then it is acceptable for Acme to have a disparate impact on protected classes.
D. If the algorithm uses information about protected classes to make automated decisions, Acme must ensure that the algorithm does not have a disparate impact on protected classes in the output.
Answer: D (LEAVE A REPLY)
The correct answer is D. If the algorithm uses information about protected classes to make automated decisions, Acme must ensure that the algorithm does not have a disparate impact on protected classes in the output. The Fair Credit Reporting Act (FCRA) protects consumers from unfair, inaccurate, and discriminatory treatment by creditors and other businesses that use credit reports. The FCRA prohibits creditors from using information about protected classes, such as race, color, religion, national origin, sex, marital status, age, or because they receive income from a public assistance program, to make decisions about credit. In the case of Acme Student Loan Company, the algorithm is using information about protected classes to make automated decisions about whether to send payment reminder calls. This could have a disparate impact on protected classes, such as people of color or people with low incomes. For example, people of color may be more

likely to be identified as being at risk of default, even if they are just as likely to repay their loans as people of other races. Acme Student Loan Company must ensure that the algorithm does not have a disparate impact on protected classes. This could be done by using a variety of methods, such as:
* Testing the algorithm for accuracy, fairness, and bias before and after deployment
* Providing consumers with notice and consent options for the use of their data
* Allowing consumers to access, correct, or delete their data
* Implementing accountability and oversight mechanisms for the algorithm
* Ensuring compliance with applicable laws and regulations
References: https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns- surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms
https://pupuweb.com/iapp-cipp-us-qa-privacy-concerns-acme-student-loan-company-artificial-intelligence/

NEW QUESTION: 170
In 2014, Google was alleged to have violated the Family Educational Rights and Privacy Act (FERPA) through its Apps for Education suite of tools. For what specific practice did students sue the company?
A. Scanning emails sent to and received by students
B. Making student education records publicly available
C. Relying on verbal consent for a disclosure of education records
D. Disclosing education records without obtaining required consent
Answer: A (LEAVE A REPLY)
The lawsuit, filed in 2014, claimed that Google violated the federal and state wiretap and privacy laws by scanning and indexing the emails of millions of students who used its Apps for Education suite, which included Gmail as a key feature. The plaintiffs alleged that Google used the information from the scans to build profiles of students that could be used for targeted advertising or other commercial purposes, without their consent or knowledge. The lawsuit also challenged Google's argument that the students consented to the scans when they first logged in to their accounts, saying that such consent was not valid under FERPA, which requires written consent for any disclosure of education records. Google denied the allegations and argued that the scans were necessary for providing security, spam protection, and other functionality to the users. The case was settled in 2016, with Google agreeing to change some of its practices and policies regarding the scanning of student emails.

NEW QUESTION: 171
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 (LEAVE A REPLY)
the PPA protects individuals; however, the PPA was drafted in direct response to the Zurcher decision: In 1978, the U.S. Supreme Court ruled in the case of Zurcher v. Stanford Daily that law enforcement could obtain search warrants to search newsrooms for evidence related to criminal activities. This decision raised concerns that such searches could impede the ability of journalists to do their jobs and gather information without fear of government interference.

NEW QUESTION: 172
SCENARIO
Please use the following to answer the next QUESTION
Noah is trying to get a new job involving the management of money. He has a poor personal credit rating, but he has made better financial decisions in the past two years. One potential employer, Arnie's Emporium, recently called to tell Noah he did not get a position. As part of the application process, Noah signed a consent form allowing the employer to request his credit report from a consumer reporting agency (CRA). Noah thinks that the report hurt his chances, but believes that he may not ever know whether it was his credit that cost him the job. However, Noah is somewhat relieved that he was not offered this particular position. He noticed that the store where he interviewed was extremely disorganized. He imagines that his credit report could still be sitting in the office, unsecured.
Two days ago, Noah got another interview for a position at Sam's Market. The interviewer told Noah that his credit report would be a factor in the hiring decision. Noah was surprised because he had not seen anything on paper about this when he applied.
Regardless, the effect of Noah's credit on his employability troubles him, especially since he has tried so hard to improve it. Noah made his worst financial decisions fifteen years ago, and they led to bankruptcy. These were decisions he made as a young man, and most of his debt at the time consisted of student loans, credit card debt, and a few unpaid bills - all of which Noah is still working to pay off. He often laments that decisions he made fifteen years ago are still affecting him today.
In addition, Noah feels that an experience investing with a large bank may have contributed to his financial troubles. In 2007, in an effort to earn money to help pay off his debt, Noah talked to a customer service representative at a large investment company who urged him to purchase stocks. Without understanding the risks, Noah agreed. Unfortunately, Noah lost a great deal of money.
After losing the money, Noah was a customer of another financial institution that suffered a large security breach. Noah was one of millions of customers whose personal information was compromised. He wonders if he may have been a victim of identity theft and whether this may have negatively affected his credit.

Noah hopes that he will soon be able to put these challenges behind him, build excellent credit, and find the perfect job.
Based on the scenario, which legislation should ease Noah's worry about his credit report as a result of applying at Arnie's Emporium?
A. The Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA).
B. The Privacy Rule under the Gramm-Leach-Bliley Act (GLBA).
C. The Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA).
D. The Red Flags Rule under the Fair and Accurate Credit Transactions Act (FACTA).
Answer: C (LEAVE A REPLY)

NEW QUESTION: 173
Under state breach notification laws, which is NOT typically included in the definition of personal information?
A. State identification number
B. First and last name
C. Social Security number
D. Medical Information
Answer: B (LEAVE A REPLY)
Under state breach notification laws, personal information is typically defined as an individual's first name or first initial and last name plus one or more other data elements, such as Social Security number, state identification number, account number, medical information, etc. However, first and last name alone are not usually considered personal information, unless they are combined with other data elements that could identify the individual or compromise their security or privacy. Therefore, option B is the correct answer, as it is not typically included in the definition of personal information under state breach notification laws.

NEW QUESTION: 174
A law enforcement subpoenas the ACME telecommunications company for access to text message records of a person suspected of planning a terrorist attack. The company had previously encrypted its text message records so that only the suspect could access this data.
What law did ACME violate by designing the service to prevent access to the information by a law enforcement agency?
A. SCA
B. ECPA
C. CALEA
D. USA Freedom Act
Answer: C (LEAVE A REPLY)
The law that ACME violated by designing the service to prevent access to the information by a law enforcement agency is the Communications Assistance for Law Enforcement Act

(CALEA)1. CALEA is a federal law that requires telecommunications carriers and manufacturers of telecommunications equipment to design their equipment, facilities, and services to ensure that they have the necessarysurveillance capabilities to comply with legal requests for interception of communications2. CALEA applies to all commercial messages, including text messages, and gives law enforcement agencies the authority to subpoena the records of such communications from the service providers3. By encrypting its text message records so that only the suspect could access this data, ACME violated CALEA's duty to cooperate in the interception of communications for law enforcement purposes. References: 1: Communications Assistance for Law Enforcement Act - Wikipedia2: Home | CALEA | The Commission on Accreditation for Law Enforcement Agencies, Inc.3: Communications Assistance for Law Enforcement Act : IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 6: Law Enforcement and National Security Access, p. 177

NEW QUESTION: 175
Under state breach notification laws, which is NOT typically included in the definition of personal information?
A. Social Security number
B. Medical Information
C. First and last name
D. State identification number
Answer: B (LEAVE A REPLY)

NEW QUESTION: 176
All of the following are tasks in the "Discover" phase of building an information management program EXCEPT?
A. Understanding the laws that regulate a company's collection of information
B. Developing a process for review and update of privacy policies
C. Facilitating participation across departments and levels
D. Deciding how aggressive to be in the use of personal information
Answer: A (LEAVE A REPLY)

NEW QUESTION: 177
In March 2012, the FTC released a privacy report that outlined three core principles for companies handling consumer data. Which was NOT one of these principles?
A. Simplifying consumer choice.
B. Enhancing security measures.
C. Practicing Privacy by Design.
D. Providing greater transparency.
Answer: B (LEAVE A REPLY)

The FTC's privacy report, titled "Protecting Consumer Privacy in an Era of Rapid Change", proposed a framework for companies that collect and use consumer data. The framework consisted of three core principles: privacy by design, simplified consumer choice, and greater transparency. Privacy by design means that companies should incorporate privacy protections into their everyday business practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy. Simplified consumer choice means that companies should provide consumers with clear and easy-to-understand choices about the collection and use of their data, and respect their preferences. Greater transparency means that companies should increase the visibility and accessibility of their data practices, such as providing clear and concise privacy notices, educating consumers about the commercial datapractices, and providing consumers with access to their data. Enhancing security measures is not one of the core principles of the FTC's privacy framework, although it is a component of the privacy by design principle. References:
* IAPP CIPP/US Body of Knowledge, Section I.A.1.a
* IAPP CIPP/US Textbook, Chapter 1, pp. 13-15
* FTC Privacy Report, Executive Summary, pp. i-vii

NEW QUESTION: 178
SCENARIO
Please use the following to answer the next QUESTION
Noah is trying to get a new job involving the management of money. He has a poor personal credit rating, but he has made better financial decisions in the past two years. One potential employer, Arnie's Emporium, recently called to tell Noah he did not get a position. As part of the application process, Noah signed a consent form allowing the employer to request his credit report from a consumer reporting agency (CRA). Noah thinks that the report hurt his chances, but believes that he may not ever know whether it was his credit that cost him the job. However, Noah is somewhat relieved that he was not offered this particular position. He noticed that the store where he interviewed was extremely disorganized. He imagines that his credit report could still be sitting in the office, unsecured.
Two days ago, Noah got another interview for a position at Sam's Market. The interviewer told Noah that his credit report would be a factor in the hiring decision. Noah was surprised because he had not seen anything on paper about this when he applied.
Regardless, the effect of Noah's credit on his employability troubles him, especially since he has tried so hard to improve it. Noah made his worst financial decisions fifteen years ago, and they led to bankruptcy. These were decisions he made as a young man, and most of his debt at the time consisted of student loans, credit card debt, and a few unpaid bills - all of which Noah is still working to pay off. He often laments that decisions he made fifteen years ago are still affecting him today.
In addition, Noah feels that an experience investing with a large bank may have contributed to his financial troubles. In 2007, in an effort to earn money to help pay off his

debt, Noah talked to a customer service representative at a large investment company who urged him to purchase stocks. Without understanding the risks, Noah agreed.
Unfortunately, Noah lost a great deal of money.
After losing the money, Noah was a customer of another financial institution that suffered a large security breach. Noah was one of millions of customers whose personal information was compromised. He wonders if he may have been a victim of identity theft and whether this may have negatively affected his credit.
Noah hopes that he will soon be able to put these challenges behind him, build excellent credit, and find the perfect job.
Consumers today are most likely protected from situations like the one Noah had buying stock because of which federal action or legislation?
A. The rules under the Fair Debt Collection Practices Act.
B. The creation of the Consumer Financial Protection Bureau.
C. Federal Trade Commission investigations into "unfair and deceptive" acts or practices.
D. Investigations of "abusive" acts and practices under the Dodd-Frank Wall Street Reform and Consumer Protection Act.
Answer: (SHOW ANSWER)
The Dodd-Frank Act was established to prevent the risky financial practices that led to the 2007-2008 financial crisis, which included issues similar to Noah's experience with buying stocks without understanding the risks. The act includes provisions forconsumer protection in financial services and aims to prevent abusive practices in the financial industry

NEW QUESTION: 179
SCENARIO
Please use the following to answer the next QUESTION
Felicia has spent much of her adult life overseas, and has just recently returned to the U.S. to help her friend Celeste open a jewelry store in Californi a. Felicia, despite being excited at the prospect, has a number of security concerns, and has only grudgingly accepted the need to hire other employees. In order to guard against the loss of valuable merchandise, Felicia wants to carefully screen applicants. With their permission, Felicia would like to run credit checks, administer polygraph tests, and scrutinize videos of interviews. She intends to read applicants' postings on social media, ask Question:s about drug addiction, and solicit character references. Felicia believes that if potential employees are serious about becoming part of a dynamic new business, they will readily agree to these requirements.
Felicia is also in favor of strict employee oversight. In addition to protecting the inventory, she wants to prevent mistakes during transactions, which will require video monitoring. She also wants to regularly check the company vehicle's GPS for locations visited by employees. She also believes that employees who use their own devices for work-related purposes should agree to a certain amount of supervision.
Given her high standards, Felicia is skeptical about the proposed location of the store. She has been told that many types of background checks are not allowed under California law.

Her friend Celeste thinks these worries are unfounded, as long as applicants verbally agree to the checks and are offered access to the results. Nor does Celeste share Felicia's concern about state breach notification laws, which, she claims, would be costly to implement even on a minor scale. Celeste believes that even if the business grows a customer database of a few thousand, it's unlikely that a state agency would hassle an honest business if an accidental security incident were to occur.
In any case, Celeste feels that all they need is common sense - like remembering to tear up sensitive documents before throwing them in the recycling bin. Felicia hopes that she's right, and that all of her concerns will be put to rest next month when their new business consultant (who is also a privacy professional) arrives from North Carolina.
Which law will be most relevant to Felicia's plan to ask applicants about drug addiction?
A. The Americans with Disabilities Act (ADA).
B. The Health Insurance Portability and Accountability Act (HIPAA).
C. The Genetic Information Nondiscrimination Act of 2008.
D. The Occupational Safety and Health Act (OSHA).
Answer: (SHOW ANSWER)

NEW QUESTION: 180
According to the FTC Report of 2012, what is the main goal of Privacy by Design?
A. Obtaining consumer consent when collecting sensitive data for certain purposes
B. Establishing a system of self-regulatory codes for mobile-related services
C. Incorporating privacy protections throughout the development process
D. Implementing a system of standardization for privacy notices
Answer: C (LEAVE A REPLY)
Privacy by Design is a concept that the FTC endorsed in its 2012 report on protecting consumer privacy. It seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. It asserts that data held by an organization ultimately belongs to the consumer and organizations should ensure that data subjects are properly informed about how their data is collected and used. Privacy by Design requires companies to build in consumers' privacy protections at every stage in developing their products, including reasonable security for consumer data, limited collection and retention of such data, and reasonable procedures to promote data accuracy.

NEW QUESTION: 181
The "Consumer Privacy Bill of Rights" 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: (SHOW ANSWER)
"he 2012 White House Report contains a preface signed by President Obama and defines the "Consumer Privacy Bill of Rights" based on traditional fair information practices (FIPs)."

NEW QUESTION: 182
Based on the 2012 Federal Trade Commission report "Protecting Consumer Privacy in an Era of Rapid Change", which of the following directives is most important for businesses?
A. Announcing the tracking of online behavior for advertising purposes.
B. Integrating privacy protections during product development.
C. Allowing consumers to opt in before collecting any data.
D. Mitigating harm to consumers after a security breach.
Answer: B (LEAVE A REPLY)
According to the FTC report, the most important directive for businesses is to adopt a "privacy by design" approach, which means integrating privacy protections throughout the entire product lifecycle, from initial design to disposal. This includes implementing reasonable security measures, collecting only the data needed for a specific purpose, retaining data only as long as necessary, and safely disposing of data that is no longer needed. The FTC report also recommends that businesses provide clear and transparent privacy notices, offer consumers meaningful choices about how their data is used, and increase their accountability for data practices. References: FTC Report, IAPP CIPP/US Study Guide (p. 32-33)

NEW QUESTION: 183
Federal laws establish which of the following requirements for collecting personal information of minors under the age of 13?
A. Implied consent from a minor's parent or guardian before collecting a minor's personal information online, such as when they permit the minor to use the internet.
B. Affirmative consent from a minor's parent or guardian before collecting the minor's personal information online.
C. Implied consent from a minor's parent or guardian, or affirmative consent from the minor.

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 (LEAVE A REPLY)

NEW QUESTION: 184
Which of the following conditions would NOT be sufficient to excuse an entity from providing breach notification under state law?
A. If the data involved was encrypted.
B. If the data involved was accessed but not exported.
C. If the entity was subject to the GLBA Safeguards Rule.
D. If the entity followed internal notification procedures compatible with state law.
Answer: (SHOW ANSWER)
While compliance with the Safeguards Rule helps in preventing breaches and ensuring data security, it does not necessarily exempt an entity from having to provide breach notifications as required by state laws. State breach notification laws typically have their own criteria for when notification is required, which may include factors like the type of data compromised, the potential risk of harm to individuals, and other circumstances surrounding the breach. While following the GLBA Safeguards Rule may demonstrate a commitment to data security, it doesn't automatically override the notification obligations imposed by state laws when a data breach occurs.

NEW QUESTION: 185
What is a legal document approved by a judge that formalizes an agreement between a governmental agency and an adverse party called?
A. A consent decree
B. Stare decisis decree
C. A judgment rider
D. Common law judgment
Answer: A (LEAVE A REPLY)
A consent decree is a legal document that resolves a dispute between a governmental agency and an adverse party without admission of guilt or liability by either side. It is approved by a judge and has the force of a court order. A consent decree may include terms such as compliance, monitoring, reporting, or remediation. A consent decree is often used to settle civil enforcement actions brought by federal agencies such as the Federal Trade Commission (FTC), the Environmental Protection Agency (EPA), or the Department of Justice (DOJ). References:
* IAPP Glossary, entry for "consent decree"
* [IAPP CIPP/US Study Guide], p. 39, section 2.1.3
* [IAPP CIPP/US Body of Knowledge], p. 9, section B.1.a

NEW QUESTION: 186

Which of the following statements is most accurate in regard to data breach notifications under federal and state laws:
A. The only obligations to provide data breach notification are under state law because currently there is no federal law or regulation requiring notice for the breach of personal information.
B. When you are required to provide an individual with notice of a data breach under any state's law, you must provide the individual with an offer for free credit monitoring.
C. You must notify the Federal Trade Commission (FTC) in addition to affected individuals if over 500 individuals are receiving notice.
D. When providing an individual with required notice of a data breach, you must identify what personal information was actually or likely compromised.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 187
What was the original purpose of the Foreign Intelligence Surveillance Act?
A. To further clarify when a warrant is not required for a wiretap performed internally by the telephone company outside the suspect's home, stemming from the Olmstead v. United States decision.
B. To further define a framework for authorizing wiretaps by the executive branch for national security purposes under Article II of the Constitution.
C. To further define what information can reasonably be under surveillance in public places under the USA PATRIOT Act, such as Internet access in public libraries.
D. To further clarify a reasonable expectation of privacy stemming from the Katz v. United States decision.
Answer: (SHOW ANSWER)

NEW QUESTION: 188
Which of the following definitions best defines privacy as cited in the text and related to privacy law?
A. The desire of people to freely choose the circumstances and the degree which individuals will expose their attitudes and behavior to others.
B. The ability of an individual to not be observed or disturbed by other people.
C. The desire of people to be free from surveillance by the government or undue public attention while residing on their personal property.
D. The right of an individual or group to seclude themselves from other individuals or organizations.
Answer: A (LEAVE A REPLY)
The essential definition of privacy is the right to be let alone. It also has been defined as the desire of people to freely choose the circumstances and the degree to which individuals will expose their attitudes and behaviors to others.?

NEW QUESTION: 189
Privacy Is Hiring Inc., a CA-based company, is an online specialty recruiting firm focusing on placing privacy professionals in roles at major companies. Job candidates create online profiles outlining their experience and credentials, and can pay $19.99/month via credit card to have their profiles promoted to potential employers. Privacy Is Hiring Inc. keeps all customer data at rest encrypted on its servers.
Under what circumstances would Privacy Is Hiring Inc., need to notify affected individuals in the event of a data breach?
A. If law enforcement has completed its investigation and has authorized Privacy Is Hiring Inc. to provide the notification to clients and applicable regulators.
B. If the job candidates' credit card information and the encryption keys were among the information taken.
C. If Privacy Is Hiring Inc., reasonably believes that job candidates will be harmed by the data breach.
D. If the personal information stolen included the individuals' names and credit card pin numbers.
Answer: B (LEAVE A REPLY)
Under the California Consumer Privacy Act (CCPA), a business that collects personal information of California residents must notify them of a data breach if their personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices. However, the CCPA excludes encrypted or redacted personal information from the definition of personal information, unless the encryption key or security credential is also compromised. Therefore, Privacy Is Hiring Inc. would need to notify the affected individuals only if the encryption keys were also taken along with the credit card information, as this would render the encryption ineffective and expose the personal information to unauthorized access.

NEW QUESTION: 190
Which of the following would NOT constitute an exception to the authorization requirement under the HIPAA Privacy Rule?
A. Disclosing health information for public health activities.
B. Disclosing health information to file a child abuse report.
C. Disclosing health information needed to treat a medical emergency.
D. Disclosing health information needed to pay a third party billing administrator.
Answer: (SHOW ANSWER)
The HIPAA Privacy Rule requires covered entities to obtain an individual's written authorization for any use or disclosure of protected health information (PHI) that is not for treatment, payment, or health care operations or otherwise permitted or required by the Privacy Rule. However, there are some exceptions to the authorization requirement for certain public interest-related activities, such as disclosing health information for public

health activities, reporting child abuse, or treating a medical emergency. These exceptions are intended to balance the privacy interests of individuals with the public interest in protecting health and safety, promoting quality health care, and ensuring compliance with the law. Disclosing health information needed to pay a third party billing administrator is not one of the exceptions to the authorization requirement, as it is considered a payment activity that falls under the general rule of requiring authorization. Therefore, it is the correct answer to the question. References: Summary of the HIPAA Privacy Rule, HIPAA Exceptions, Exceptions to HIPAA Privacy Rule, Waiver of Authorization, IAPP CIPP/US Study Guide, Chapter 5.

NEW QUESTION: 191
When designing contact tracing apps in relation to COVID-19 or any other diagnosed virus, all of the following privacy measures should be considered EXCEPT?
A. Data retention.
B. Use limitations.
C. Opt-out choice.
D. User confidentiality.
Answer: (SHOW ANSWER)
Contact tracing apps are designed to help public health authorities track and contain the spread of COVID-19 or any other diagnosed virus by notifying users who have been in close contact with an infected person.
However, these apps also raise privacy concerns, as they collect and process sensitive personal data, such as health status and location information. Therefore, contact tracing apps should follow the principles of privacy by design and default, which means that they should incorporate privacy measures into their development and operation, and offer the highest level of privacy protection to users.
Some of the privacy measures that should be considered when designing contact tracing apps are:
* Data retention: Contact tracing apps should only retain the personal data they collect for as long as necessary to achieve their public health purpose, and delete or anonymize the data afterwards. Data retention periods should be clearly communicated to users and based on scientific evidence and legal requirements.
* Use limitations: Contact tracing apps should only use the personal data they collect for the specific and legitimate purpose of contact tracing, and not for any other purposes, such as commercial, law enforcement, or surveillance. Use limitations should be enforced by technical and organizational measures, such as encryption, access controls, and audits.
* User confidentiality: Contact tracing apps should protect the confidentiality of users' personal data and identity, and not disclose them to third parties without their consent or legal authorization. User confidentiality should be ensured by technical and organizational measures, such as pseudonymization, aggregation, and data minimization.

Opt-out choice, on the other hand, is not a privacy measure that should be considered when designing contact tracing apps, as it would undermine their effectiveness and public health objective. Contact tracing apps rely on voluntary participation and widespread adoption by users to function properly and achieve their purpose.
Therefore, offering users the option to opt out of the app or certain features, such as data sharing or notifications, would reduce the app's coverage and accuracy, and potentially expose users and others to greater health risks. Instead of opt-out choice, contact tracing apps should provide users with clear and transparent information about how the app works, what data it collects and how it uses it, what benefits and risks it entails, and what rights and controls users have over their data. This way, users can make an informed and voluntary decision to use the app or not, based on their own preferences and values.
References:
* [IAPP CIPP/US Study Guide], Chapter 2: Privacy by Design and Default, pp. 35-36.
* [IAPP CIPP/US Body of Knowledge], Section II: Limits on Private-sector Collection and Use of Data, Subsection B: Privacy by Design, pp. 9-10.
* [IAPP Glossary], Terms: Contact Tracing, Privacy by Design, Privacy by Default.

NEW QUESTION: 192
In 2011, the FTC announced a settlement with Google regarding its social networking service Google Buzz. The FTC alleged that in the process of launching the service, the company did all of the following EXCEPT?
A. Violated its own privacy policies.
B. Engaged in deceptive trade practices.
C. Failed to comply with Safe Harbor principles.
D. Failed to employ sufficient security safeguards.
Answer: D (LEAVE A REPLY)
https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz-social-network

NEW QUESTION: 193
The U.S. Supreme Court has recognized an individual's right to privacy over personal issues, such as contraception, by acknowledging which of the following?
A. Federal preemption of state constitutions that expressly recognize an individual right to privacy.
B. A "penumbra" of unenumerated constitutional rights as well as more general protections of due process of law.
C. An interpretation of the U.S. Constitution's explicit definition of privacy that extends to personal issues.
D. The doctrine of stare decisis, which allows the U.S. Supreme Court to follow the precedent of previously decided case law.
Answer: B (LEAVE A REPLY)

The U.S. Supreme Court has recognized an individual's right to privacy over personal issues, such as contraception, by acknowledging a "penumbra" of unenumerated constitutional rights as well as more general protections of due process of law. This means that the right to privacy is not explicitly stated in the Constitution, but it is implied from other rights that are explicitly stated, such as the First Amendment rights of speech and assembly, the Third Amendment right to be free from quartering of soldiers, the Fourth Amendment right to be secure from unreasonable searches and seizures, the Fifth Amendment right to be free from self-incrimination, and the Ninth Amendment right to retain other rights not enumerated in the Constitution. These rights create a "zone of privacy" that protects individuals from undue government interference in their personal affairs. The Supreme Court first articulated this concept of privacy in Griswold v. Connecticut (1965), where it struck down a state law that prohibited the use of contraceptives by married couples. The Court also relied on the due process clause of the Fourteenth Amendment, which prohibits states from depriving any person of life, liberty, or property without due process of law. The Court interpreted this clause to include a substantive component that protects certain fundamental rights from state regulation, unless there is a compelling state interest and the regulation is narrowly tailored to achieve that interest. The Court has applied this due process analysis to other privacy issues, such as abortion, marriage, and sexual orientation. References:
* Privacy | Wex | US Law | LII / Legal Information Institute
* Privacy isn't in the Constitution - but it's everywhere in constitutional law
* Privacy Rights and Personal Autonomy Legally Protected by the ... - Justia
* Right to privacy | Wex | US Law | LII / Legal Information Institute

NEW QUESTION: 194
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 Red Flags Rule by mailing the reports to customers
B. To follow the Safeguards Rule by transferring the reports to a secure electronic file
C. To follow the Privacy Rule by notifying customers that the reports are being stored
D. To follow the Disposal Rule by having the reports shredded
Answer: C (LEAVE A REPLY)

NEW QUESTION: 195
Which action is prohibited under the Electronic Communications Privacy Act of 1986?
A. Monitoring employee telephone calls of a personal nature
B. Intercepting electronic communications and unauthorized access to stored communications
C. Accessing stored communications with the consent of the sender or recipient of the message
D. Monitoring all employee telephone calls

Answer: (SHOW ANSWER)
The Electronic Communications Privacy Act of 1986 (ECPA) is a federal law that protects the privacy of wire, oral, and electronic communications while they are being made, in transit, or stored on computers. The ECPA has three titles: Title I prohibits the intentional interception, use, or disclosure of wire, oral, or electronic communications, except for certain exceptions, such as consent, provider protection, or law enforcement purposes. Title II, also known as the Stored Communications Act (SCA), prohibits the unauthorized access to or disclosure of stored wire or electronic communications, such as email, voicemail, or online messages, except for certain exceptions, such as consent, provider protection, or law enforcement purposes. Title III regulates the installation and use of pen register and trap and trace devices, which record the numbers dialed to or from a telephone line, but not the content of the communications. Therefore, the action that is prohibited under the ECPA is intercepting electronic communications and unauthorized access to stored communications, which are covered by Title I and Title II of the Act, respectively.

NEW QUESTION: 196
Privacy Is Hiring Inc., a CA-based company, is an online specialty recruiting firm focusing on placing privacy professionals in roles at major companies. Job candidates create online profiles outlining their experience and credentials, and can pay $19.99/month via credit card to have their profiles promoted to potential employers. Privacy Is Hiring Inc. keeps all customer data at rest encrypted on its servers.
Under what circumstances would Privacy Is Hiring Inc., need to notify affected individuals in the event of a data breach?
A. If law enforcement has completed its investigation and has authorized Privacy Is Hiring Inc. to provide the notification to clients and applicable regulators.
B. If the job candidates' credit card information and the encryption keys were among the information taken.
C. If Privacy Is Hiring Inc., reasonably believes that job candidates will be harmed by the data breach.
D. If the personal information stolen included the individuals' names and credit card pin numbers.
Answer: B (LEAVE A REPLY)
California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (California Civil Code s. 1798.29(a) [agency] and California Civ. Code s. 1798.82(a) [person or business].)
https://oag.ca.gov/privacy/databreach/reporting

NEW QUESTION: 197
Which of the following scenarios would NOT be covered under HIPAA?
A. Doctor visit for annual physical
B. Chemotherapy related to cancer treatment in a medical facility
C. Billing codes, patient name, and insurance identification sent to an insurance company for payment
D. Medical books purchased through Amazon
Answer: D (LEAVE A REPLY)
It is important to understand that HIPAA applies to these covered entities, but not to other healthcare providers and services. Individuals surfing the web or purchasing books about healthcare are not covered by HIPAA.

NEW QUESTION: 198
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 (LEAVE A REPLY)
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.

NEW QUESTION: 199
Which of the following types of information would an organization generally NOT be required to disclose to law enforcement?
A. Information about medication errors under the Food, Drug and Cosmetic Act
B. Money laundering information under the Bank Secrecy Act of 1970
C. Information about workspace injuries under OSHA requirements
D. Personal health information under the HIPAA Privacy Rule
Answer: D (LEAVE A REPLY)
The HIPAA Privacy Rule generally prohibits covered entities and business associates from disclosing protected health information (PHI) to law enforcement without the individual's authorization, unless one of the exceptions in 45 CFR § 164.512 applies. These exceptions include disclosures required by law, disclosures for law enforcement purposes, disclosures about victims of abuse, neglect or domestic violence, disclosures for health oversight activities, disclosures for judicial and administrative proceedings, disclosures for research purposes, disclosures to avert a serious threat to health or safety, disclosures for specialized government functions, disclosures for workers' compensation, and disclosures to coroners and medical examiners. None of these exceptions apply to the type of information in option D, which is personal health information that is not related to any of the above purposes. Therefore, an organization would generally not be required to disclose such information to law enforcement under the HIPAA Privacy Rule. References:
https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties
https://bing.com/search?q=information+disclosure+to+law+enforcement
https://hipaatrek.com/law-enforcement-hipaa-disclosing-phi/

NEW QUESTION: 200
SCENARIO
Please use the following to answer the next question:
Noah is trying to get a new job involving the management of money. He has a poor personal credit rating, but he has made better financial decisions in the past two years. One potential employer, Arnie's Emporium, recently called to tell Noah he did not get a position.

As part of the application process, Noah signed a consent form allowing the employer to request his credit report from a consumer reporting agency (CRA). Noah thinks that the report hurt his chances, but believes that he may not ever know whether it was his credit that cost him the job.
However, Noah is somewhat relieved that he was not offered this particular position. He noticed that the store where he interviewed was extremely disorganized. He imagines that his credit report could still be sitting in the office, unsecured.
Two days ago, Noah got another interview for a position at Sam's Market. The interviewer told Noah that his credit report would be a factor in the hiring decision. Noah was surprised because he had not seen anything on paper about this when he applied.
Regardless, the effect of Noah's credit on his employability troubles him, especially since he has tried so hard to improve it. Noah made his worst financial decisions fifteen years ago, and they led to bankruptcy. These were decisions he made as a young man, and most of his debt at the time consisted of student loans, credit card debt, and a few unpaid bills ?all of which Noah is still working to pay off. He often laments that decisions he made fifteen years ago are still affecting him today.
In addition, Noah feels that an experience investing with a large bank may have contributed to his financial troubles. In 2007, in an effort to earn money to help pay off his debt, Noah talked to a customer service representative at a large investment company who urged him to purchase stocks. Without understanding the risks, Noah agreed.
Unfortunately, Noah lost a great deal of money.
After losing the money, Noah was a customer of another financial institution that suffered a large security breach. Noah was one of millions of customers whose personal information was compromised. He wonders if he may have been a victim of identity theft and whether this may have negatively affected his credit.
Noah hopes that he will soon be able to put these challenges behind him, build excellent credit, and find the perfect job.
Based on the scenario, which legislation should ease Noah's worry about his credit report as a result of applying at Arnie's Emporium?
A. The Privacy Rule under the Gramm-Leach-Bliley Act (GLBA).
B. The Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA).
C. The Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA).
D. The Red Flags Rule under the Fair and Accurate Credit Transactions Act (FACTA).
Answer: (SHOW ANSWER)
The Department of Commerce (DOC) plays a role in privacy policy by promoting the development and adoption of voluntary codes of conduct, standards, and best practices for the private sector, as well as facilitating cross-border data transfers through mechanisms such as the EU-U.S.
Privacy Shield and the APEC Cross-Border Privacy Rules. However, the DOC does not have regulatory authority to enforce privacy laws or impose sanctions for privacy violations. The other agencies listed have some degree of regulatory authority over privacy issues

within their respective domains. For example, the Office of the Comptroller of the Currency (OCC) supervises national banks and federal savings associations and enforces the GLBA privacy and security rules for these institutions. The Federal Communications Commission (FCC) regulates interstate and international communications and enforces the privacy and security rules for telecommunications carriers, broadband providers, and voice over internet protocol (VoIP) services. The Department of Transportation (DOT) oversees the transportation sector and enforces the privacy and security rules for airlines, travel agents, and other covered entities under the Aviation and Transportation Security Act (ATSA).

NEW QUESTION: 201
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 ignoring the conversation about a potential breach
B. By speaking to a patient without prior authorization
C. By being present when patients are checking in
D. By following through with his plans for his upcoming paper
Answer: (SHOW ANSWER)

NEW QUESTION: 202
What type of material is exempt from an individual's right to disclosure under the Privacy Act?
A. Material reporting investigative efforts pertaining to the enforcement of criminal law.
B. Material requires by statute to be maintained and used solely for research purposes.
C. Material used to determine potential collaboration with foreign governments in negotiation of trade deals.
D. Material reporting investigative efforts to prevent unlawful persecution of an individual.
Answer: (SHOW ANSWER)

NEW QUESTION: 203
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 (LEAVE A REPLY)
* Implied consent is a form of consent that is inferred from the actions or inactions of the data subject, rather than explicitly expressed by the data subject1.
* Implied consent is generally considered a valid basis for processing personal data under certain circumstances, such as when the processing is necessary for the performance of a contract, the legitimate interests of the data controller, or the reasonable expectations of the data subject2.

* However, implied consent may not be sufficient for processing sensitive personal data, such as health, biometric, or genetic data, or for sending marketing communications, depending on the applicable laws and regulations2.
* In the U.S., there is no comprehensive federal privacy law that regulates the use of implied consent for data processing, but there are sector-specific laws and state laws that may impose different requirements and limitations3.
* Based on the scenarios given in the question, the situation that is most likely to involve a company operating under the assumption of implied consent is A. An employer contacts the professional references provided on an applicant's resume.
* This is because the employer may reasonably infer that the applicant has consented to the contact of the references by voluntarily providing their information on the resume, and that the contact is necessary for the legitimate interest of the employer to verify the applicant's qualifications and suitability for the job4.
* The other situations may not involve implied consent, but rather require explicit consent or provide opt- out options for the data subjects, depending on the type and purpose of the data processing and the relevant laws and regulations5 . For example:
* B. An online retailer subscribes new customers to an e-mail list by default. This may violate the CAN-SPAM Act, which requires online marketers to obtain affirmative consent from the recipients before sending commercial e-mail messages, and to provide a clear and conspicuous opt-out mechanism in every message5.
* C. A landlord uses the information on a completed rental application to run a credit report. This may violate the Fair Credit Reporting Act, which requires landlords to obtain written authorization from the applicants before obtaining their consumer reports, and to provide them with a copy of the report and a summary of their rights if they take any adverse action based on the report.
* D. A retail clerk asks a customer to provide a zip code at the check-out counter. This may violate the California Song-Beverly Credit Card Act, which prohibits retailers from requesting and recording personal identification information from customers who pay with a credit card, unless the information is necessary for a special purpose, such as shipping or fraud prevention.
References: 1: Implied Consent 2: Consent 3: U.S. Private-Sector Privacy (CIPP/US) 4: [Reference Checks:
Tips for Job Applicants and Employers] 5: [CAN-SPAM Act: A Compliance Guide for Business] : [Using Consumer Reports: What Landlords Need to Know] : [California Song-Beverly Credit Card Act] : [Reference Checks: Tips for Job Applicants and Employers] : [CAN-SPAM Act: A Compliance Guide for Business] :
[Using Consumer Reports: What Landlords Need to Know] : [California Song-Beverly Credit Card Act]

NEW QUESTION: 204

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 (LEAVE A REPLY)

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.

NEW QUESTION: 205

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

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 (LEAVE A REPLY)

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 seizures. 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 belongings. 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 government. 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 circumstances.

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.

NEW QUESTION: 206
Which of the following would NOT be regulated by the Illinois Biometnc Information Pnvacy Act (BIPA)?
A. Photographs of local convicted felons uploaded lo a news website.
B. Fingerprint scans of elementary school students used to open their lockers
C. Security software designed to identify local convicted felons in retail stores via facial recognition.
D. Retina scans of elementary school students used to verify their identities for attendance purposes
Answer: A (LEAVE A REPLY)
The Illinois Biometric Information Privacy Act (BIPA) regulates the collection, storage, and use of biometric identifiers and biometric information, such as fingerprints, retina scans, and facial recognition data.
However, BIPA does not regulate photographs, as they are explicitly excluded from the definition of
"biometric identifiers" under the law.
Key Definitions Under BIPA:
* Biometric Identifier:Includes fingerprints, retina or iris scans, voiceprints, and scans of hand or face geometry.
* Biometric Information:Refers to any information derived from biometric identifiers.
* Exclusions:BIPA explicitly excludes certain types of data from regulation, such as photographs, writing samples, and physical descriptions.
Explanation of Options:
* A. Photographs of local convicted felons uploaded to a news website:This is correct because photographs are explicitly excluded from BIPA's definition of biometric identifiers.
* B. Fingerprint scans of elementary school students used to open their lockers:This would be regulated under BIPA, as fingerprints are considered biometric identifiers.

* C. Security software designed to identify local convicted felons in retail stores via facial recognition:This would also be regulated under BIPA, as facial recognition involves scans of face geometry, which qualify as biometric identifiers.
* D. Retina scans of elementary school students used to verify their identities for attendance purposes:Retina scans are biometric identifiers under BIPA and would therefore be regulated.
References from CIPP/US Materials:
* Illinois BIPA (740 ILCS 14/10): Defines biometric identifiers and excludes photographs from regulation.
* IAPP CIPP/US Certification Textbook: Discusses the scope and application of BIPA.

NEW QUESTION: 207
Which statement is FALSE regarding the provisions of the Employee Polygraph Protection Act of
1988 (EPPA)?
A. The EPPA requires that employers post essential information about the Act in a conspicuous location.
B. The EPPA includes an exception that allows polygraph tests in professions in which employee honesty is necessary for public safety.
C. Employers are prohibited from administering psychological testing based on personality traits such as honesty, preferences or habits.
D. Employers involved in the manufacture of controlled substances may terminate employees based on polygraph results if other evidence exists.
Answer: (SHOW ANSWER)
The false statement regarding the provisions of the EPPA is C. Employers are prohibited from administering psychological testing based on personality traits such as honesty, preferences or habits. The EPPA does not regulate psychological testing, only polygraph testing. Psychological testing is a broad term that covers various types of assessments that measure cognitive abilities, personality traits, interests, values, and skills. Employers may use psychological testing for various purposes, such as hiring, promotion, training, or development, as long as they comply with other laws and regulations, such as the Americans with Disabilities Act (ADA), the Equal Employment Opportunity Commission (EEOC) guidelines, and the Uniform Guidelines on Employee Selection Procedures. However, employers should be careful to ensure that the psychological tests they use are valid, reliable, job-related, and nondiscriminatory, and that they respect the privacy and dignity of the test takers.

NEW QUESTION: 208
Which of the following best describes how federal anti-discrimination laws protect the privacy of private-sector employees in the United States?
A. They prescribe working environments that are safe and comfortable.

B. They limit the amount of time a potential employee can be interviewed.
C. They promote a workforce of employees with diverse skills and interests.
D. They limit the types of information that employers can collect about employees.
Answer: D (LEAVE A REPLY)
Federal anti-discrimination laws, such as Title VII of the Civil Rights Act of 1964, the Equal Pay Act of 1963, the Age Discrimination in Employment Act of 1967, and the Americans with Disabilities Act of 1990, prohibit employers from discriminating against employees or applicants based on certain protected characteristics, such as race, color, religion, sex, national origin, age, disability, and genetic information. These laws also limit the types of information that employers can collect, use, disclose, or retain about employees or applicants,in order to prevent discrimination or invasion of privacy. For example, employers cannot ask about an applicant's medical history, disability status, genetic information, or religious beliefs, unless they are relevant to the job or a bona fide occupational qualification. Employers also cannot use such information to make adverse employment decisions, such as hiring, firing, promotion, or compensation, unless they are justified by a legitimate business necessity or a reasonable accommodation. Employers must also safeguard the confidentiality of such information and dispose of it properly when it is no longer needed. References:
* Federal Laws Prohibiting Job Discrimination Questions And Answers
* Laws Enforced by EEOC
* Employment and Anti-Discrimination Laws in the Workplace
* Protections Against Discrimination and Other Prohibited Practices
* 3. Who is protected from employment discrimination?

NEW QUESTION: 209
Which of the following is an important implication of the Dodd-Frank Wall Street Reform and Consumer Protection Act?
A. Financial institutions must avoid collecting a customer's sensitive personal information
B. Financial institutions must help ensure a customer's understanding of products and services
C. Financial institutions must use a prescribed level of encryption for most types of customer records
D. Financial institutions must cease sending e-mails and other forms of advertising to customers who opt out of direct marketing
Answer: B (LEAVE A REPLY)
The Dodd-Frank Act created the Consumer Financial Protection Bureau (CFPB) as an independent agency within the Federal Reserve System. The CFPB has the authority to regulate consumer financial products and services, such as mortgages, credit cards, student loans, and payday loans. One of the main objectives of the CFPB is to promote transparency, fairness, and consumer choice in the financial marketplace. The CFPB has issued rules and guidance to require financial institutions to provide clear and accurate

information to consumers about the costs, risks, and benefits of their products and services. The CFPB also has the power to enforce consumer protection laws and prohibit unfair, deceptive, or abusive acts or practices by financial institutions.

NEW QUESTION: 210
Which of the following practices is NOT a key component of a data ethics framework?
A. Automated decision-making.
B. Preferability testing.
C. Data governance.
D. Auditing.
Answer: A (LEAVE A REPLY)
A data ethics framework is a set of principles and guidelines that help organizations ensure that their data practices are ethical, responsible, and trustworthy. According to the IAPP CIPP/US Study Guide, some of the key components of a data ethics framework are1:
* Data governance: the policies, processes, and standards that govern how data is collected, used, stored, and shared within an organization.
* Preferability testing: the process of assessing the potential impacts and risks of data-driven solutions on stakeholders, such as customers, employees, and society.
* Auditing: the process of monitoring, reviewing, and verifying the compliance and performance of data practices against the established ethical standards and legal requirements. Automated decision-making, on the other hand, is not a key component of a data ethics framework, but rather a data practice that may raise ethical issues and challenges. Automated decision-making refers to the use of algorithms, artificial intelligence, or machine learning to make decisions or recommendations without human intervention2. While automated decision-making can offer benefits such as efficiency, accuracy, and consistency, it can also pose risks such as bias, discrimination, lack of transparency, and accountability3. Therefore, automated decision-making should be subject to ethical evaluation and oversight, but it is not itself a part of a data ethics framework. References:
* [IAPP CIPP/US Study Guide], Chapter 10, Section 10.4, page 287
* [IAPP Glossary], Automated Decision-Making
* IAPP Resources, Ethical Data Use and Automated Decision-Making: A Practical Guide

NEW QUESTION: 211
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.

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

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: (SHOW ANSWER)

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. References:

* 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.

NEW QUESTION: 212
Which venture would be subject to the requirements of Section 5 of the Federal Trade Commission Act?
A. A local nonprofit charity's fundraiser
B. An online merchant's free shipping offer
C. A national bank's no-fee checking promotion
D. A city bus system's frequent rider program
Answer: B (LEAVE A REPLY)
Section 5 of the Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices in or affecting commerce."1 This prohibition applies to all persons engaged in commerce, including banks, but also exempts some entities, such as nonprofit organizations and common carriers, from FTC jurisdiction.2 Therefore, among the four options, only an online merchant's free shipping offer would be subject to the requirements of Section 5, as it involves a commercial activity thatcould potentially mislead or harm consumers. For example, if the online merchant fails to disclose the terms and conditions of the offer, or charges hidden fees, or delivers the products late or damaged, it could violate Section 5 by engaging in a deceptive practice.3 References: 1: Section 5 | Federal Trade Commission 2: Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices, page 13: IAPP CIPP/US Certified Information Privacy Professional Study Guide, page 23.

NEW QUESTION: 213
Which venture would be subject to the requirements of Section 5 of the Federal Trade Commission Act?
A. A local nonprofit charity's fundraiser
B. An online merchant's free shipping offer
C. A national bank's no-fee checking promotion
D. A city bus system's frequent rider program
Answer: (SHOW ANSWER)
Section 5 of the Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices in or affecting commerce."1 This prohibition applies to all persons

engaged in commerce, including banks, but also exempts some entities, such as nonprofit organizations and common carriers, from FTC jurisdiction.
2 Therefore, among the four options, only an online merchant's free shipping offer would be subject to the requirements of Section 5, as it involves a commercial activity that could potentially mislead or harm consumers. For example, if the online merchant fails to disclose the terms and conditions of the offer, or charges hidden fees, or delivers the products late or damaged, it could violate Section 5 by engaging in a deceptive practice.3 References: 1: Section 5 | Federal Trade Commission 2: Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices, page 13: IAPP CIPP/US Certified Information Privacy Professional Study Guide, page 23.

NEW QUESTION: 214
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 (LEAVE A REPLY)
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 exceptions1. 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 crimes12. 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 so12. 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. References: 1: FERPA, 34 CFR Part 99, Subpart D, 2. 2: The Family Educational Rights and Privacy Act Guidance for Parents, Student Privacy Policy Office, U.S. Department of Education, 1.

NEW QUESTION: 215
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 (LEAVE A REPLY)
The Red Flag Program Clarification Act of 2010 amended the original Red Flags rule, which required certain financial institutions and creditors to develop and implement a written identity theft prevention program. The Clarification Act narrowed the definition of creditor to include only those who regularly and in the ordinary course of business advance funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person. This excludes creditors who advance funds for expenses incidental to a service provided by the creditor to that person.

NEW QUESTION: 216
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.
Based on the incident, the FTC's enforcement actions against the marketer would most likely include what violation?
A. Intruding upon the privacy of a family with young children.
B. Failing to notify of a breach of children's private information.
C. Disregarding the privacy policy of the children's marketing industry.

D. Collecting information from a child under the age of thirteen.
Answer: (SHOW ANSWER)

NEW QUESTION: 217
In what way does the "Red Flags Rule" under the Fair and Accurate Credit Transactions Act (FACTA) relate to the owner of a grocery store who uses a money wire service?
A. It mandates the use of updated technology for securing credit records
B. It requires the owner to implement an identity theft warning system
C. It is not usually enforced in the case of a small financial institution
D. It does not apply because the owner is not a creditor
Answer: D (LEAVE A REPLY)
The Red Flags Rule is a regulation that requires financial institutions and creditors to implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account1. A creditor is any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit2. A covered account is an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account2. A money wire service is a service that allows customers to send or receive money electronically3. The owner of a grocery store who uses a money wire service is not a creditor because he or she does not regularly extend, renew, or continue credit to customers. Therefore, the Red Flags Rule does not apply to the owner of a grocery store who uses a money wire service. References:
* 1: FTC, Red Flags Rule, https://www.ftc.gov/business-guidance/privacy-security/red-flags-rule
* 2: FTC, Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business, https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-
* 3: Alessa, Wire Transfer Red Flags: Understanding Money Laundering and Fraud Risks, https://alessa.com/webinars/wire-transfer-red-flags-and-fraud-risks/