IAPP.CIPP-US.v2022-06-20.q69

Exam Code:	CIPP-US
Exam Name:	Certified Information Privacy Professional/United States (CIPP/US)
Certification Provider:	IAPP
Free Question Number:	69
Version:	v2022-06-20
# of views:	3896
# of Questions views:	3220
https://www.dumpsfiles.com/files/IAPP/CIPP-US/IAPP.CIPP-US.v2022-06-20.q69	

NEW QUESTION: 1
An organization self-certified under Privacy Shield must, upon request by an individual, do what?
A. Suspend the use of all personal information collected by the organization to fulfill its original purpose.
B. Provide the identities of third parties with whom the organization shares personal information.
C. Provide the identities of third and fourth parties that may potentially receive personal information.
D. Identify all personal information disclosed during a criminal investigation.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
https://www.lakesidesoftware.com/sites/default/files/Privacy_Shield_Privacy_Statement.pdf

NEW QUESTION: 2
John, a California resident, receives notification that a major corporation with $500 million in annual revenue has experienced a data breach. John's personal information in their possession has been stolen, including his full name and social security numb. John also learns that the corporation did not have reasonable cybersecurity measures in place to safeguard his personal information.
Which of the following answers most accurately reflects John's ability to pursue a legal claim against the corporation under the California Consumer Privacy Act (CCPA)?
A. John cannot sue the corporation for the data breach because only the state's Attoney General has authority to file suit under the CCPA.

B. John can sue the corporation for the data breach to recover monetary damages suffered as a result of the data breach, and in some circumstances seek statutory damages irrespective of whether he suffered any financial harm.
C. John has no right to sue the corporation because the CCPA does not address any data breach rights.
D. John can sue the corporation for the data breach but only to recover monetary damages he actually suffered as a result of the data breach.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
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 exercise control over how companies use their personal data.
B. Consumers have a right to correct personal data in a manner that is appropriate to the sensitivity.
C. Consumers have a right to reasonable limits on the personal data that a company retains.
D. Consumers have a right to easily accessible information about privacy and security practices.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
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 CloudHealth violated its contract with HealthCo by not encrypting the ePHI
C. Because HIPAA requires the imposition of a fine if a data breach of this magnitude has occurred
D. Because HealthCo did not conduct due diligence to verify or monitor CloudHealth's security measures
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
Smith Memorial Healthcare (SMH) is a hospital network headquartered in New York and operating in 7 other states. SMH uses an electronic medical record to enter and track information about its patients. Recently, SMH suffered a data breach where a third-party hacker was able to gain access to the SMH internal network.
Because it is a HIPPA-covered entity, SMH made a notification to the Office of Civil Rights at the U.S. Department of Health and Human Services about the breach.
Which statement accurately describes SMH's notification responsibilities?
A. If SMH is compliant with HIPAA, it will not have to make a separate notification to individuals in the state of New York.
B. If SMH has more than 500 patients in the state of New York, it will need to make separate notifications to these patients.
C. If SMH must make a notification in any other state in which it operates, it must also make a notification to individuals in New York.
D. If SMH makes credit monitoring available to individuals who inquire, it will not have to make a separate
Answer: C (LEAVE A REPLY)
notification to individuals in the state of New York.

NEW QUESTION: 6
Which of the following is NOT a principle found in the APEC Privacy Framework?
A. Privacy by Design.
B. Preventing Harm.
C. Integrity of Personal Information.
D. Access and Correction.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 7
In which situation is a company operating under the assumption of implied consent?
A. A landlord uses the information on a completed rental application to run a credit report
B. An online retailer subscribes new customers to an e-mail list by default
C. An employer contacts the professional references provided on an applicant's resume

D. A retail clerk asks a customer to provide a zip code at the check-out counter
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
The Family Educational Rights and Privacy Act (FERPA) requires schools to do all of the following EXCEPT?
A. Provide students with access to their records within a specified amount of time.
B. Obtain student authorization before releasing directory information in their records.
C. Verify the identity of students who make requests for access to their records.
D. Respond to all reasonable student requests regarding explanation of their records.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
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 what area does Larry have a misconception about private-sector employee rights?
A. The applicability of federal law
B. The enforceability of local law
C. The strict nature of state law
D. The definition of tort law
Answer: A (LEAVE A REPLY)

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. Correct their personal information.
B. Disclose their personal information to them.
C. Refrain from selling their personal information to third parties.
D. Delete their personal information.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
Which entity within the Department of Health and Human Services (HHS) is the primary enforcer of the Health Insurance Portability and Accountability Act (HIPAA) "Privacy Rule"?
A. Office for Civil Rights.
B. Office of Social Services.
C. Office of Public Health and Safety.
D. Office of Inspector General.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
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 baseline of marketers' minimum responsibilities for providing opt-out mechanisms.
C. A code of responsibilities for medical establishments to uphold privacy laws.
D. A bill of rights for individuals seeking access to their personal information.
Answer: (SHOW ANSWER)

NEW QUESTION: 13
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 types of information that employers can collect about employees.
C. They limit the amount of time a potential employee can be interviewed.
D. They promote a workforce of employees with diverse skills and interests.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
What practice does the USA FREEDOM Act NOT authorize?
A. Emergency exceptions that allows the government to target roamers
B. An increase in the maximum penalty for material support to terrorism
C. An extension of the expiration for roving wiretaps
D. The bulk collection of telephone data and internet metadata
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.rand.org/blog/2015/05/the-usa-freedom-act-the-definition-of-a-compromise.html

NEW QUESTION: 15
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)
Explanation/Reference:
https://www.healthaffairs.org/do/10.1377/hblog20150304.045199/full/

NEW QUESTION: 16
How did the Fair and Accurate Credit Transactions Act (FACTA) amend the Fair Credit Reporting Act (FCRA)?
A. It stipulated the purpose of obtaining a consumer report can only be for a review of the employee's credit worthiness
B. It expanded the definition of "consumer reports" to include communications relating to employee investigations
C. It increased the obligation of organizations to dispose of consumer data in ways that prevent unauthorized access
D. It required employers to get an employee's consent in advance of requesting a consumer report for internal investigation purposes Section: (none) Explanation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
A covered entity suffers a ransomware attack that affects the personal health information (PHI) of more than 500 individuals. According to Federal law under HIPAA, which of the following would the covered entity NOT have to report the breach to?
A. Department of Health and Human Services
B. The affected individuals
C. The local media
D. Medical providers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
Who has rulemaking authority for the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA)?
A. State Attorneys General
B. The Federal Trade Commission
C. The Department of Commerce
D. The Consumer Financial Protection Bureau
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003

NEW QUESTION: 19
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 clarify a reasonable expectation of privacy stemming from the Katz v. United States decision.
D. 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.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
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)
Explanation/Reference: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

NEW QUESTION: 21
What information did the Red Flag Program Clarification Act of 2010 add to the original Red Flags rule?
A. The components of an identity theft detection program.
B. The definition of what constitutes a creditor.
C. The process for proper disposal of sensitive data.
D. The most common methods of identity theft.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
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. Marketing (such as appending data to customer information that a marketing company already has).
D. Risk mitigation (such as information that may reduce the risk of fraud).
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
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 employee training program
B. The vendor's employee retention rates
C. The vendor's financial health
D. The vendor's reputation
Answer: (SHOW ANSWER)

NEW QUESTION: 24

All of the following organizations are specified as covered entities under the Health Insurance Portability and Accountability Act (HIPAA) EXCEPT?
A. Health plans
B. Healthcare providers
C. Healthcare information clearinghouses
D. Pharmaceutical companies
Answer: D (LEAVE A REPLY)

NEW QUESTION: 25
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.
Regarding credit checks of potential employees, Celeste has a misconception regarding what?
A. Employment-at-will rules.
B. Consent requirements.

C. Records retention policies
D. Disclosure requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Sarah lives in San Francisco, Californi
a. 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. 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.
B. The California Consumer Privacy Act entitles Sarah to request deletion of her personal information.
C. Any company with a presence in Europe must comply with the General Data Protection Regulation globally, including in response to data subject deletion requests.
D. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
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 Occupational Safety and Health Act (OSHA).
B. The Americans with Disabilities Act (ADA).
C. The Genetic Information Nondiscrimination Act of 2008.
D. The Health Insurance Portability and Accountability Act (HIPAA).
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
California's SB 1386 was the first law of its type in the United States to do what?
A. Require notification of non-California residents of a breach that occurred in California
B. Require commercial entities to disclose a security data breach concerning personal information about the state's residents
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: (SHOW ANSWER)

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.
What is the best reason for Cheryl to follow Janice's suggestion about classifying customer data?
A. It will help employees stay better organized
B. It will help the company meet a federal mandate
C. It will increase the security of customers' personal information (PI)
D. It will prevent the company from collecting too much personal information (PI)
Answer: (SHOW ANSWER)
Explanation/Reference:
https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/dcps/

NEW QUESTION: 30
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 is still a dependent for tax purposes
B. If the student has not yet turned 18 years of age
C. If the student has applied to transfer to another institution
D. If the student is in danger of academic suspension
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
What is a key way that the Gramm-Leach-Bliley Act (GLBA) prevents unauthorized access into a person's back account?
A. By restricting the disclosure of customer account numbers by financial institutions.
B. By requiring the amount of customer personal information printed on paper.
C. By requiring the financial institutions limit the collection of personal information.
D. By requiring immediate public disclosure after a suspected security breach.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
An organization self-certified under Privacy Shield must, upon request by an individual, do what?
A. Identify all personal information disclosed during a criminal investigation.
B. Provide the identities of third parties with whom the organization shares personal information.
C. Provide the identities of third and fourth parties that may potentially receive personal information.
D. Suspend the use of all personal information collected by the organization to fulfill its original purpose.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
U.S. federal laws protect individuals from employment discrimination based on all of the following EXCEPT?
A. Genetic information.
B. Age.
C. Pregnancy.
D. Marital status.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34

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)
Explanation
Explanation/Reference: https://www.nap.edu/read/11896/chapter/11#283

NEW QUESTION: 35
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.
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 only applies to companies based in California, which exempts the company from compliance.

B. That the company is governed by CCPA, but does not need to take any additional steps because it follows CPBR.
C. That CCPA will apply to the company only after the California Attorney General determines that it will enforce the statute.
D. That business contact information could be considered personal information governed by CCPA.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
When may a financial institution share consumer information with non-affiliated third parties for marketing purposes?
A. After disclosing marketing practices to customers and after giving them an opportunity to opt out.
B. After disclosing information-sharing 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 in.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
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: 38
When does the Telemarketing Sales Rule require an entity to share a do-not-call request across its organization?
A. When a call is not the result of an error or other unforeseen cause
B. When the operational structures of its divisions are not transparent
C. When the goods and services sold by its divisions are very similar
D. When the entity manages user preferences through multiple platforms
Answer: (SHOW ANSWER)

NEW QUESTION: 39

What consumer protection did the Fair and Accurate Credit Transactions Act (FACTA) require?
A. Consumer notice when third-party data is used to make an adverse decision
B. The truncation of account numbers on credit card receipts
C. The right to request removal from e-mail lists
D. The ability for the consumer to correct inaccurate credit report information
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
Which of the following accurately describes the purpose of a particular federal enforcement agency?
A. The Federal Trade Commission (FTC) is typically recognized as having the broadest authority under the FTC Act to address unfair or deceptive privacy practices.
B. 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).
C. The Federal Communications Commission (FCC) regulates privacy practices on the internet and enforces violations relating to websites' posted privacy disclosures.
D. 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.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
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 used to determine potential collaboration with foreign governments in negotiation of trade deals.
C. Material reporting investigative efforts to prevent unlawful persecution of an individual.
D. Material reporting investigative efforts pertaining to the enforcement of criminal law.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
Which action is prohibited under the Electronic Communications Privacy Act of 1986?
A. Accessing stored communications with the consent of the sender or recipient of the message
B. Monitoring all employee telephone calls
C. Intercepting electronic communications and unauthorized access to stored communications
D. Monitoring employee telephone calls of a personal nature

Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
In 2012, the White House and the FTC both issued reports advocating a new approach to privacy enforcement that can best be described as what?
A. Comprehensive.
B. Harm-based.
C. Self-regulatory.
D. Notice and choice.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44
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: (SHOW ANSWER)

NEW QUESTION: 45
Which of the following laws is NOT involved in the regulation of employee background checks?
A. The California Investigative Consumer Reporting Agencies Act (ICRAA).
B. The U.S. Fair Credit Reporting Act (FCRA).
C. The Civil Rights Act.
D. The Gramm-Leach-Bliley Act (GLBA).
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
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 Red Flags Rule under the Fair and Accurate Credit Transactions Act (FACTA).
D. The Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA).

Answer: (SHOW ANSWER)

NEW QUESTION: 47
A covered entity suffers a ransomware attack that affects the personal health information (PHI) of more than
500 individuals. According to Federal law under HIPAA, which of the following would the covered entity NOT have to report the breach to?
A. Department of Health and Human Services
B. The affected individuals
C. The local media
D. Medical providers
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (page 6)

NEW QUESTION: 48
What is the main challenge financial institutions face when managing user preferences?
A. Developing a mechanism for opting out that is easy for their consumers to navigate
B. Ensuring they are in compliance with numerous complex state and federal privacy laws
C. Determining the legal requirements for sharing preferences with their affiliates
D. Ensuring that preferences are applied consistently across channels and platforms
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 50
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.
Based on the way he uses social media, Evan is susceptible to a lawsuit based on?
A. Discrimination
B. Intrusion upon seclusion
C. Publicity given to private life
D. Defamation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 51
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 video monitors in physical locations, such as a changing room, to reduce the risk of sexual harassment.
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 a video monitor in physical locations, such as a warehouse, to ensure employees are performing tasks in a safe manner and environment.
D. An employer who records all employee phone calls that involve financial transactions with customers completed over the phone.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
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. CALEA
B. USA Freedom Act
C. ECPA
D. SCA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 53
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)
Explanation/Reference: https://www.varonis.com/blog/ccpa-vs-gdpr/

NEW QUESTION: 54
Which of the following is NOT a principle found in the APEC Privacy Framework?
A. Integrity of Personal Information.

B. Access and Correction.
C. Preventing Harm.
D. Privacy by Design.
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiqtJX4tPHvAhUQG-wKHUoGBgkQFjAHegQIBRAD&url=https%3A%2F%2Fwww.apec.org%2F-%2Fmedia%2FAPEC%2FPublications%2F2016%2F11%2F2016-CTI-Report-to-Ministers%2FTOC%2FAppendix-17-Updates-to-the- APEC-Privacy-Framework.pdf&usg=AOvVaw1Ysi4Ym_1VaCw1VZiB70a

NEW QUESTION: 55
Which is an exception to the general prohibitions on telephone monitoring that exist under the U.S. Wiretap Act?
A. Inter-company communications exception
B. Call center exception
C. Ordinary course of business exception
D. Internet calls exception
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
Which of the following is most likely to provide privacy protection to private-sector employees in the United States?
A. State law, contract law, and tort law
B. The Federal Trade Commission Act (FTC Act)
C. Amendments one, four, and five of the U.S. Constitution
D. The U.S. Department of Health and Human Services (HHS)
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://corporate.findlaw.com/law-library/right-to-privacy-in-the-workplace-in-the-information- age.html

NEW QUESTION: 57
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 Privacy Is Hiring Inc., reasonably believes that job candidates will be harmed by the data breach.
B. If law enforcement has completed its investigation and has authorized Privacy Is Hiring Inc. to provide the notification to clients and applicable regulators.
C. If the personal information stolen included the individuals' names and credit card pin numbers.
D. If the job candidates' credit card information and the encryption keys were among the information taken.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 58
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. Human rights may be disregarded for the sake of privacy
C. Industries may not be strict enough in the creation and enforcement of rules
D. A new business owner may not understand the regulations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
Global Manufacturing Co's Human Resources department recently purchased a new software tool. This tool helps evaluate future candidates for executive roles by scanning emails to see what those candidates say and what is said about them. This provides the HR department with an automated "360 review" that lets them know how the candidate thinks and operates, what their peers and direct reports say about them, and how well they interact with each other.
What is the most important step for the Human Resources Department to take when implementing this new software?
A. Making sure that the software does not unintentionally discriminate against protected groups.
B. Ensuring that the software contains a privacy notice explaining that employees have no right to privacy as long as they are running this software on organization systems to scan email systems.
C. Confirming that employees have read and signed the employee handbook where they have been advised that they have no right to privacy as long as they are using the organization's systems, regardless of the protected group or laws enforced by EEOC.
D. Providing notice to employees that their emails will be scanned by the software and creating automated profiles.
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.beckage.com/tag/artificial-intelligence/

NEW QUESTION: 60
Which statute is considered part of U.S. federal privacy law?
A. The Fair Credit Reporting Act.
B. SB 1386.
C. The Personal Information Protection and Electronic Documents Act.
D. The e-Privacy Directive.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
Most states with data breach notification laws indicate that notice to affected individuals must be sent in the
"most expeditious time possible without unreasonable delay." By contrast, which of the following states currently imposes a definite limit for notification to affected individuals?
A. Maine
B. Florida
C. New York
D. California
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://www.itgovernanceusa.com/data-breach-notification-laws

NEW QUESTION: 62
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: 63
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 conduct due diligence to verify or monitor CloudHealth's security measures

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

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

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 64

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 contain the number to which calls can be made and must have an end date

B. The consent must be in writing, must state the times when calls can be made to the consumer and must be signed
C. The consent must be in writing, must have an end data and must state the times when calls can be made
D. The consent must be in writing, must contain the number to which calls can be made and must be signed
Answer: (SHOW ANSWER)

NEW QUESTION: 65
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. Information about workspace injuries under OSHA requirements
C. Money laundering information under the Bank Secrecy Act of 1970
D. Personal health information under the HIPAA Privacy Rule
Answer: D (LEAVE A REPLY)

NEW QUESTION: 66
What are banks required to do under the Gramm-Leach-Bliley Act (GLBA)?
A. Offer an Opt-Out before transferring PI to an unaffiliated third party for the latter's own use
B. Conduct annual consumer surveys regarding satisfaction with user preferences
C. Provide consumers with the opportunity to opt out of receiving telemarketing phone calls
D. Process requests for changes to user preferences within a designated time frame
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67
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)
Reference:
~klett/chapter%25202%2520bl281%2520judicial%2520review%2520new.htm
+&cd=1&hl=en&ct=clnk&gl=pk&client=firefox-b-e

NEW QUESTION: 68
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 CloudHealth's HR policy regarding the role of employees involved data breaches
D. Training on the difference between confidential and non-public information
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
Which federal law or regulation preempts state law?
A. Electronic Communications Privacy Act of 1986
B. Telemarketing Sales Rule
C. Health Insurance Portability and Accountability Act
D. Controlling the Assault of Non-Solicited Pornography and Marketing Act

Answer: C (LEAVE A REPLY)