CIPP-US.VCEplus.premium.exam.107q

Number: CIPP-US
Passing Score: 800
Time Limit: 120 min
File Version: 2.0

CIPP/US

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

Version 2.0

Exam A

QUESTION 1

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://webcache.googleusercontent.com/search?q=cache:kG3AN4srIh8J:https://www.shsu.edu/~klett/chapter%25202%2520bl281%2520judicial%2520review%2520new.htm+&cd=1&hl=en&ct=clnk&gl=pk&client=firefox-b-e

QUESTION 2 Which authority supervises and enforces laws regarding advertising to children via the Internet?

A. The Office for Civil Rights
B. The Federal Trade Commission
C. The Federal Communications Commission
D. The Department of Homeland Security

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/sites/default/files/documents/public_statements/advertising-kids-and-ftc-regulatory-retrospective-advises-present/040802adstokids.pdf

QUESTION 3
According to Section 5 of the FTC Act, self-regulation **primarily** involves a company's right to do what?

A. Determine which bodies will be involved in adjudication
B. Decide if any enforcement actions are justified
C. Adhere to its industry's code of conduct
D. Appeal decisions made against it

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

QUESTION 4 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

Correct Answer: A
Section: (none)

Explanation
Explanation/Reference:
Reference: https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

QUESTION 5
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

QUESTION 6
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Read this notice:

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

What type of legal choice does not notice provide?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8 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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/dcps/

QUESTION 9 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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 10 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 **main** problem with Cheryl's suggested method of communicating the new privacy policy?

A. The policy would not be considered valid if not communicated in full.
B. The policy might not be implemented consistency across departments.
C. Employees would not be comfortable with a policy that is put into action over time.
D. Employees might not understand how the documents relate to the policy as a whole.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Global_Privacy_Enforcement_Network

QUESTION 15
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.edweek.org/ew/articles/2014/03/13/26google.h33.html

QUESTION 16 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.lakesidesoftware.com/sites/default/files/Privacy_Shield_Privacy_Statement.pdf

QUESTION 18
Which of the following federal agencies does **NOT** enforce the Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA)?

A. The Office of the Comptroller of the Currency
B. The Consumer Financial Protection Bureau
C. The Department of Health and Human Services
D. The Federal Trade Commission

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Fair_and_Accurate_Credit_Transactions_Act

QUESTION 19 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 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.

Upon review, the data privacy leader discovers that the Company's documented data inventory is obsolete. What is the data privacy leader's next best source of information to aid the investigation?

A. Reports on recent purchase histories
B. Database schemas held by the retailer
C. Lists of all customers, sorted by country
D. Interviews with key marketing personnel

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.i-scoop.eu/gdpr/data-processor-gdpr/

QUESTION 22 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: https://privacyproficient.com/what-is-no-option-or-no-consumer-choice/

QUESTION 24 What is the **main** challenge financial institutions face when managing user preferences?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Implied_consent

QUESTION 27
All of the following are tasks in the "Discover" phase of building an information management program EXCEPT?

A. Facilitating participation across departments and levels
B. Developing a process for review and update of privacy policies
C. Deciding how aggressive to be in the use of personal information
D. Understanding the laws that regulate a company's collection of information

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
If an organization certified under Privacy Shield wants to transfer personal data to a third party acting as an agent, the organization must ensure the third party does all of the following EXCEPT?

A. Uses the transferred data for limited purposes
B. Provides the same level of privacy protection as the organization
C. Notifies the organization if it can no longer meet its requirements for proper data handling
D. Enters a contract with the organization that states the third party will process data according to the consent agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.privacyshield.gov/Key-New-Requirements

QUESTION 30 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/about-ftc

QUESTION 31 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. Collecting information from a child under the age of thirteen.
C. Failing to notify of a breach of children’s private information.
D. Disregarding the privacy policy of the children’s marketing industry.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/system/files/2012-31341.pdf

QUESTION 32 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 does Matt come to the decision to report the marketer’s activities?

A. The marketer failed to make an adequate attempt to provide Matt with information
B. The marketer did not provide evidence that the prize books were appropriate for children
C. The marketer seems to have distributed his son’s information without Matt’s permissionD. The marketer failed to identify himself and indicate the purpose of the messages

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/system/files/2012-31341.pdf

QUESTION 33 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/system/files/2012-31341.pdf

QUESTION 34
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.healthaffairs.org/do/10.1377/hblog20150304.045199/full/

QUESTION 35
All of the following organizations are specified as covered entities under the Health Insurance Portability and Accountability Act (HIPAA) EXCEPT?

A. Healthcare information clearinghouses
B. Pharmaceutical companies
C. Healthcare providers
D. Health plans

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

QUESTION 36
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (page 6)

QUESTION 37 What consumer protection did the Fair and Accurate Credit Transactions Act (FACTA) require?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.investopedia.com/terms/f/facta.asp

QUESTION 38
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003

QUESTION 39
Under the Fair and Accurate Credit Transactions Act (FACTA), what is the **most** appropriate action for a car dealer holding a paper folder of customer credit reports?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

QUESTION 41 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.investopedia.com/terms/g/glba.asp

QUESTION 42 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule

QUESTION 46
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47 When does the Telemarketing Sales Rule require an entity to share a do-not-call request across its organization?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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 daysC. 15 days
D. 21 days

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

QUESTION 49
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpafaq.pdf

QUESTION 50
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 54
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

QUESTION 55 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://searchcompliance.techtarget.com/definition/Video-Privacy-Protection-Act-of-1988

QUESTION 56
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.fcc.gov/media/engineering/cable-television

QUESTION 57 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58 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 occurredD. Because CloudHealth violated its contract with HealthCo by not encrypting the ePHI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 59 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 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.

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
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61 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.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 64
What practice do courts commonly require in order to protect certain personal information on documents, whether paper or electronic, that is involved in litigation?

A. Redaction
B. Encryption
C. Deletion
D. Hashing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/electronic-communications-privacy-act

QUESTION 66 What was the original purpose of the Foreign Intelligence Surveillance Act?

A. 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.
B. To further clarify a reasonable expectation of privacy stemming from the Katz v. United States decision.
C. To further define a framework for authorizing wiretaps by the executive branch for national security purposes under Article II of the Constitution.
D. 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://epic.org/privacy/surveillance/fisa/

QUESTION 67
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.rand.org/blog/2015/05/the-usa-freedom-act-the-definition-of-a-compromise.html

QUESTION 68 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1057&context=nulr

QUESTION 69 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which is an exception to the general prohibitions on telephone monitoring that exist under the U.S. Wiretap Act?

A. Call center exception
B. Inter-company communications exception
C. Ordinary course of business exception
D. Internet calls exception

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.lexology.com/library/detail.aspx?g=1031d6a6-19f5-4422-b5a2-98d7038905e9

QUESTION 72 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 media. 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73 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 media. 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. Defamation
B. Discrimination
C. Intrusion upon seclusion
D. Publicity given to private life

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74 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 media. 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 Whistleblower Protection Act
B. The Stored Communications Act (SCA)
C. The National Labor Relations Act (NLRA)
D. The Fair and Accurate Credit Transactions Act (FACTA)

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 75 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 media. 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 conditions under which recipients can opt out
B. The wishes of recipients who request callbacks
C. The right to monitor calls for quality assurance
D. The relationship of state law to federal law

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.worktime.com/what-are-the-u-s-employee-monitoring-laws-get-updated-in-2020

QUESTION 77
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)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://corporate.findlaw.com/law-library/right-to-privacy-in-the-workplace-in-the-information-age.html

QUESTION 78 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79 Which action is prohibited under the Electronic Communications Privacy Act of 1986?

A. Intercepting electronic communications and unauthorized access to stored communications
B. Monitoring all employee telephone calls
C. Accessing stored communications with the consent of the sender or recipient of the message
D. Monitoring employee telephone calls of a personal nature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

QUESTION 80 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/interviewandemploymentapplicationquestions.aspx

QUESTION 81 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which federal law or regulation preempts state law?
A. Health Insurance Portability and Accountability Act
B. Controlling the Assault of Non-Solicited Pornography and Marketing Act
C. Telemarketing Sales Rule
D. Electronic Communications Privacy Act of 1986

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/system/files/documents/public_comments/2014/11/00098-92984.pdf (3)

QUESTION 87
What does the Massachusetts Personal Information Security Regulation require as it relates to encryption of personal information?

A. The encryption of all personal information of Massachusetts residents when all equipment is located in Massachusetts.
B. The encryption of all personal information stored in Massachusetts-based companies when all equipment is located in Massachusetts.
C. The encryption of personal information stored in Massachusetts-based companies when stored on portable devices.
D. The encryption of all personal information of Massachusetts residents when stored on portable devices.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.dataguidance.com/notes/massachusetts-data-protection-overview

QUESTION 88 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://corporate.findlaw.com/law-library/california-raises-the-bar-on-data-security-and-privacy.html

QUESTION 89
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.itgovernanceusa.com/data-breach-notification-laws

QUESTION 90
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

QUESTION 91 Which of the following **best** describes what a "private right of action" is?

A. The right of individuals to keep their information private.
B. The right of individuals to submit a request to access their information.
C. The right of individuals harmed by data processing to have their information deleted.
D. The right of individuals harmed by a violation of a law to file a lawsuit against the violation.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://iapp.org/resources/article/private-right-of-action/

QUESTION 92
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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=AOvVaw1Yysi4Ym_1VaCw1VZiB70a

QUESTION 93
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://iapp.org/news/a/what-does-the-ccpas-purpose-limitation-mean-for-businesses/

QUESTION 94 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.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96 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.

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Reference: http://documents1.worldbank.org/curated/en/751621525705087132/text/WPS8431.txt

QUESTION 97
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.natlawreview.com/article/ringing-2019-new-state-privacy-and-data-security-laws-impacting-data-brokers-and

QUESTION 98
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms

QUESTION 99
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 lawsenforced by EEOC.
D. Providing notice to employees that their emails will be scanned by the software and creating automated profiles.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.beckage.com/tag/artificial-intelligence/

QUESTION 100
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103 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. DefamationD. Conversion.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Privacy_law

QUESTION 104
Which law provides employee benefits, but often mandates the collection of medical information?
A. The Occupational Safety and Health Act.
B. The Americans with Disabilities Act.
C. The Employee Medical Security Act.
D. The Family and Medical Leave Act.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.dph.illinois.gov/covid19/community-guidance/workplace-health-and-safety-guidance/employee-employer-rights-and-safety

QUESTION 105
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 has no right to sue the corporation because the CCPA does not address any data breach rights.
B. John cannot sue the corporation for the data breach because only the state's Attoney General has authority to file suit under the CCPA.
C. 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.
D. 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Smith Memorial Healthcare (SMH) is a hospital network headquartered in New York and operating in 7 other states. SMH uses an electronic medical record to enter and track information about its patients. Recently, SMH suffered a data breach where a third-party hacker was able to gain access to the SMH internal network. Because it is a HIPPA-covered entity, SMH made a notification to the Office of Civil Rights at the U.S. Department of Health and Human Services about the breach.

Which statement accurately describes SMH's notification responsibilities?

A. If SMH is compliant with HIPAA, it will not have to make a separate notification to individuals in the state of New York.
B. If SMH has more than 500 patients in the state of New York, it will need to make separate notifications to these patients.
C. If SMH must make a notification in any other state in which it operates, it must also make a notification to individuals in New York.
D. If SMH makes credit monitoring available to individuals who inquire, it will not have to make a separate notification to individuals in the state of New York.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.varonis.com/blog/ccpa-vs-gdpr/