Number: CIPP-US
Passing Score: 800.0
Time Limit: 120.0
File Version: 9.0

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

Exam A

QUESTION 1
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:
Explanation:
https://es.vccs.edu/about/family-educational-rights-and-privacy-act-ferpa/ The disclosure is to a parent who legally declares the student as a dependent, as defined by 20 U.S.C. 1232g. (NOTE: Regardless of the student's age, a parent seeking access to their son or daughter's educational record must present proof upon each request of their child's dependency to the Registrar's Office by way of the most recent year's federal tax return.)

QUESTION 2
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: D
Section:
Explanation:
https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business#who

QUESTION 3
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:

QUESTION 4
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:

QUESTION 5
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:

QUESTION 6
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:

QUESTION 7
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: A
Section:
Explanation:
'The Disposal Rule requires any individual or entity that uses a consumer report, or information derived from a consumer report, for a business purpose to dispose of that consumer information in a way that prevents unauthorized access and misuse of the data. Consumer reports can be electronic or written. The rule applies to both small and large organizations, including consumer reporting agencies, lenders, employers, insurers, landlords, car dealers, attorneys, debt collectors, and government agencies.' and 'Examples of acceptable, reasonable measures include developing and complying with policies to: Burn, pulverize or shred papers containing consumer report information so that the information cannot be read or reconstructed Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the rule'

QUESTION 8

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:
Explanation:
https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act 'If you share their NPI with nonaffiliated third parties outside of three exceptions (see 'Exceptions'), you must give your consumers and customers an 'opt-out notice' that clearly and conspicuously describes their right to opt out of the information being shared. An opt-out notice must be delivered with a privacy notice, and it can be part of the privacy notice.'

QUESTION 9
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:

QUESTION 10
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: D
Section:
Explanation:
'Other than for treatment, covered entities must make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary in order to accomplish the intended purpose.' He isn't involved in the potential breach, which is why he isn't trained for it, and doesn't know all the facts of the situation. He has not obligation doesn't need to investigate any further based on anything that he heard.

QUESTION 11
SCENARIO
Please use the following to answer the next QUESTION :
Declan has just started a job as a nursing assistant in a radiology department at Woodland Hospital. He has also started a program to become a registered nurse.
Before taking this career path, Declan was vaguely familiar with the Health Insurance Portability and Accountability Act (HIPAA). He now knows that he must help ensure the security of his patients' Protected Health Information (PHI). Therefore, he is thinking carefully about privacy issues.
On the morning of his first day, Declan noticed that the newly hired receptionist handed each patient a HIPAA privacy notice. He wondered if it was necessary to give these privacy notices to returning patients, and if the radiology department could reduce paper waste through a system of one-time distribution.
He was also curious about the hospital's use of a billing company. He Questioned whether the hospital was doing all it could to protect the privacy of its patients if the billing company had details about patients' care.
On his first day Declan became familiar with all areas of the hospital's large radiology department. As he was organizing equipment left in the halfway, he overheard a conversation between two hospital administrators. He was surprised to hear that a portable hard drive containing non-encrypted patient information was missing. The administrators expressed relief that the hospital would be able to avoid liability. Declan was surprised, and wondered whether the hospital had plans to properly report what had happened.
Despite Declan's concern about this issue, he was amazed by the hospital's effort to integrate Electronic Health Records (EHRs) into the everyday care of patients. He thought about the potential for streamlining care even more if they were accessible to all medical facilities nationwide.
Declan had many positive interactions with patients. At the end of his first day, he spoke to one patient, John, whose father had just been diagnosed with a degenerative muscular disease. John was about to get blood work done, and he feared that the blood work could reveal a genetic predisposition to the disease that could affect his ability to obtain insurance coverage. Declan told John that he did not think that was possible, but the patient was wheeled away before he could explain why. John plans to ask a colleague about this.
In one month, Declan has a paper due for one his classes on a health topic of his choice. By then, he will have had many interactions with patients he can use as examples. He will be pleased to give credit to John by name for inspiring him to think more carefully about genetic testing.
Although Declan's day ended with many QUESTIONS, he was pleased about his new position.
How can the radiology department address Declan's concern about paper waste and still comply with the Health Insurance Portability and Accountability Act (HIPAA)?

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

Correct Answer: C
Section:
Explanation:
It is important for test takers to not add additional information to the prompt by assuming information. By choosing D, you are assuming that Declan will stay long enough in the position that he will personally see to it that every first time patient receives a privacy notice. By choosing C, you are answering the exact question by addressing the paper waste concern and complying with HIPAA which allows covered entities to post privacy notices on websites. Model Notices of Privacy Practices on the HHS website outlines two requirements: A covered entity must make its notice available to any person who asks for it (satisfies pointing the person in the direction of the covered entity website); A covered entity must prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits (satisfies pointing the person to the covered entity website to view privacy notice).

QUESTION 12
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:

QUESTION 13
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: A
Section:
Explanation:
Some types of businesses are not covered by the TSR even though they conduct telemarketing campaigns that may involve some interstate telephone calls to sell goods or services. These three types of entities are not subject to the FTC's jurisdiction, and are not covered by the TSR:
1. banks, federal credit unions, and federal savings and loans.
2. common carriers --- such as long-distance telephone companies and airlines --- when they are engaging in common carrier activity.
3. NON-PROFIT ORGANIZATIONS --- those entities that are not organized to carry on business for their own, or their members', profit.
https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#comply

QUESTION 14
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: C
Section:
Explanation:
https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement What must the written agreement contain? A written agreement need only contain: - unambiguous evidence that a call recipient is willing to receive telephone calls that deliver a - prerecorded message by or on behalf of a specific seller; the telephone number to which such messages may be delivered; and - the call recipient's signature.

QUESTION 15
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:

QUESTION 16
Within what time period must a commercial message sender remove a recipient's address once they have asked to stop receiving future e-mail?

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

Correct Answer: B
Section:

QUESTION 17
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:

QUESTION 18
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:

QUESTION 19
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: A
Section:

QUESTION 20
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:

QUESTION 21
SCENARIO
Please use the following to answer the next QUESTION :
You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures. A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals -- ones that exposed the PHI of public figures including celebrities and politicians. During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected. A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach. What is the most significant reason that the U.S. Department of Health and Human Services (HHS) might impose a penalty on HealthCo?

A. Because HealthCo did not require CloudHealth to implement appropriate physical and administrative measures to safeguard the ePHI
B. Because HealthCo did not conduct due diligence to verify or monitor CloudHealth's security measures
C. Because HIPAA requires the imposition of a fine if a data breach of this magnitude has occurred

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

Correct Answer: B
Section:

QUESTION 22
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:

QUESTION 23
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: C
Section:
Explanation:
Section 8.1.2 of the textbook lists the Security Rule Safeguards as admin, technical and physical. Security safeguards are not considered one of the three categories.

QUESTION 24
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: B
Section:

QUESTION 25
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:
Explanation:
These are 'permissive' disclosures. The covered entity or business associate may refuse. https://www.eff.org/issues/law-enforcement-

QUESTION 26
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:
Explanation:
To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes.

QUESTION 27
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:

QUESTION 28
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: A
Section:
Explanation:
https://wyattfirm.com/the-electronic-communications-privacy-act-of-1986-tracking-the-productivity-of-work-from-home-employees/ 'In other words, monitoring must be relevant to the business, recurring, and the employee must know about it.' Here it is personal and there is no indication that the employee knew.

QUESTION 29
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: C
Section:

QUESTION 30
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: D
Section:
Explanation:
'The USA FREEDOM Act ended bulk collection conducted under Section 215.154 Going forward, requests by government officials must be based upon specific selectors, such as a telephone number. Company officials are now permitted to release statistics about the number of such requests they receive in a given time period, and the government is required to report its numbers once a year.155 In 2018, government officials obtained 56 court orders for traditional business records and 14 court orders for call detail records.156'

QUESTION 31
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: A
Section:
Explanation:
the PPA protects individuals; however, the PPA was drafted in direct response to the Zurcher decision: In 1978, the U.S. Supreme Court ruled in the case of Zurcher v. Stanford Daily that law enforcement could obtain search warrants to search newsrooms for evidence related to criminal activities. This decision raised concerns that such searches could impede the ability of journalists to do their jobs and gather information without fear of government interference.

QUESTION 32
The rules for ''e-discovery'' mainly prevent which of the following?

A. A conflict between business practice and technological safeguards
B. The loss of information due to poor data retention practices
C. The practice of employees using personal devices for work
D. A breach of an organization's data retention program

Correct Answer: B
Section:
Explanation:
Page 346 of the learning material - '.....e-discovery rules, which require automated and large-scale production of emails and other corporate documents during the discovery process prior to trial'.

QUESTION 33
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:

QUESTION 34
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:

QUESTION 35
SCENARIO
Please use the following to answer the next QUESTION :
Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. ''If they were really serious about not being bothered,'' Evan said, ''They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to.''
Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call ''another time.'' This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.
Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social medi a. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.
Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.
Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
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:

QUESTION 36
SCENARIO
Please use the following to answer the next QUESTION :
Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. ''If they were really serious about not being bothered,'' Evan said, ''They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to.''
Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call ''another time.'' This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.
Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects

American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social medi a. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.
Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.
Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
Based on the way he uses social media, Evan is susceptible to a lawsuit based on?

A. Defamation
B. Discrimination
C. Intrusion upon seclusion
D. Publicity given to private life

Correct Answer: B
Section:

QUESTION 37
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: D
Section:
Explanation:
The U.S. Constitution has signicant workplace privacy provisions that apply to the federal and state governments, but they do not affect private-sector employment. Notably, the Fourth Amendment prohibits unreasonable searches and seizures by state actors. Courts have interpreted this amendment to place limits on the ability of government employers to search employees' private spaces, such as lockers and desks.4 Some states, including California, have extended their constitutional rights to privacy to private-sector employees.5 In general for private-sector actors, however, there is no state action, and no constitutional law governs employment privacy

QUESTION 38
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:

QUESTION 39
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:

QUESTION 40
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:
Explanation:
Section: (none)
Explanation:

QUESTION 41
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:

QUESTION 42
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:

QUESTION 43
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: C
Section:

QUESTION 44
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: B
Section:

QUESTION 45
SCENARIO
Please use the following to answer the next QUESTION :
Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. ''If they were really serious about not being bothered,'' Evan said, ''They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to.''
Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call ''another time.'' This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.
Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social medi a. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.
Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.
Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
Which act would authorize Evan's undercover investigation?

A. The 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: B
Section:
Explanation:
Stored communications. As previously discussed, the SCA creates a general prohibition against the unauthorized acquisition, alteration or blocking of electronic communications while in electronic storage in a facility through which an electronic communications service is provided.119 Violations for interceptions can lead to criminal penalties or a civil lawsuit. The law provides for exceptions. Two exceptions that may apply to the employer are for

conduct authorized: ''By the person or entity providing a wire or electronic communications service'' (often the employer)120 ''By a user of that service with respect to a communication of or intended for that user''121

QUESTION 46
SCENARIO
Please use the following to answer the next QUESTION :
Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. ''If they were really serious about not being bothered,'' Evan said, ''They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to.''
Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call ''another time.'' This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.
Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social medi a. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.
Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.
Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
In regard to telemarketing practices, Evan the supervisor has a misconception regarding?

A. The 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:

QUESTION 47
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:

QUESTION 48
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:

QUESTION 49
The use of cookies on a website by a service provider is generally not deemed a 'sale' of personal information by CCPA, as long as which of the following conditions is met?

A. The third party stores personal information to trigger a response to a consumer's request to exercise their right to opt in.
B. The analytics cookies placed by the service provider are capable of being tracked but cannot be linked to a particular consumer of that business.
C. The service provider retains personal information obtained in the course of providing the services specified in the agreement with the subcontractors.
D. The information collected by the service provider is necessary to perform debugging and the business and service provider have entered into an appropriate agreement.

Correct Answer: C
Section:

QUESTION 50
Under the Driver's Privacy Protection Act (DPPA), which of the following parties would require consent of an individual in order to obtain his or her Department of Motor Vehicle information?

A. Law enforcement agencies performing investigations.
B. Insurance companies needing to investigate claims.
C. Attorneys gathering information related to lawsuits.
D. Marketers wishing to distribute bulk materials.

Correct Answer: D
Section:
Explanation:
https://dmv.ny.gov/forms/mv15dppa.pdf

QUESTION 51
Which of the following federal agencies does NOT have regulatory authority related to privacy?

A. Consumer Financial Protection Bureau.
B. U.S. Department of Transportation.
C. U.S. Department of Commerce.
D. Federal Reserve

Correct Answer: B
Section:

QUESTION 52
Which of the following practices is NOT a key component of a data ethics framework?

A. Automated decision-making.
B. Preferability testing.
C. Data governance.
D. Auditing.

Correct Answer: B
Section:

QUESTION 53
What was unique about the action that the Federal Trade Commission took against B.J.'s Wholesale Club in 2005?

A. It made third-party audits a penalty for policy violations.
B. It was based on matters of fairness rather than deception.
C. It was the first substantial U.S.-EU Safe Harbor enforcement.
D. It made user consent mandatory after any revisions of policy.

Correct Answer: B
Section:
Explanation:
Per the FTC Press Release in 2005, 'BJ's Wholesale Club, Inc. has agreed to settle Federal Trade Commission charges that its failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice that violated federal law.'