CIPP/US Sample Questions

Practice questions are indispensable for good exam preparation. Below you will find thirty IAPP style CIPP/US practice questions including two scenario questions.

The sample questions are part of our CIPP/US online training course. Our courses contain more than 300 of these practice questions. More information can be found at CIPPTraining.com.

1. Which of the following definitions best defines privacy as cited in the text and related to privacy law?

   A. The desire of people to freely choose the circumstances and the degree which individuals will expose their attitudes and behavior to others.
   B. The ability of an individual to not be observed or disturbed by other people.
   C. The desire of people to be free from surveillance by the government or undue public attention while residing on their personal property.
   D. The right of an individual or group to seclude themselves from other individuals or organizations.

2. In most cases, the FTC settles disputes through consent decrees and consent orders. What is the maximum length of a consent decree?

   A. 5 years
   B. 10 years
   C. 20 years
   D. Indefinitely

3. Which step in developing an Information Management Program involves distributing privacy policies and privacy notices?

   A. Build
   B. Communicate
   C. Discover
   D. Regulate

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

   A. Data Mapping
   B. Data Classification
   C. Data Flow Documentation
   D. Data Protection Laws

5. Which of the following would NOT fall under the jurisdiction of the GDPR?

   A. A German company with assets in France and employees in both companies.
   B. An Italian company selling products and services worldwide.
   C. A Spanish company that processes data of US citizens.
   D. A US company who sells products and services in South America.

6. Which form of malicious online threat targets an individual user and pretends to be a legitimate party, such as a bank, to steal personal data?

A. Spear Phishing
B. Ransomware
C. Technical Based Attack
D. Hacking

7. Which of the following entities is the PRIMARY enforcer of the HIPAA Privacy Rule and can assess civil monetary penalties?

A. Federal Trade Commission
B. Office of Civil Rights
C. State Attorney General
D. US Department of Justice

8. Which legislation provides privacy provisions for the exemption of disclosure of certain biomedical information, securing remote access to view PHI, prohibiting the blocking of information, certificates of confidentiality, and compassionate sharing of mental health or substance abuse information with family or caregivers?

A. 21st Century Cures Act of 2016
B. GINA of 2008
C. HITECH of 2013
D. HIPAA Security Rule of 2003

9. Who is responsible for notifying consumers when adverse action is taken based on information in a consumer credit report?

A. The Credit Bureau
B. The User
C. The Credit Reporting Agency
D. The Consumer Financial Protection Bureau

10. Which two FCRA rules were added with the Fair and Accurate Credit Transitions Act in 2003?

A. Disposal Rule and Red Flags Rule
B. Privacy Rule and Safeguards Rule
C. Disposal Rule and Safeguards Rule
D. Privacy Rule and Red Flags Rule

Use the following scenario to answer questions 11-15.

Select the BEST answer for each question. Some answers may be partly correct, but only one answer is the best.

Don lives in California with his wife and two children. Sarah is 12 years old and in the 7th grade at her school. Robert is 15 and a Sophomore at his school. Don is concerned about his children and their online activities as they use social media and talk with their friends.

Sarah has an Xbox One that she primarily uses to stream content from Netflix, Hulu, and YouTube, but she does play a few games on the system too. Robert has a PlayStation 4 and is an avid gamer. He loves cooperative multiplayer games with his friends. Sarah and Robert each received their gaming consoles as a gift from their parents last year. Upon first use, both had to setup user profiles and input some basic information.

11. According to the Children's Online Privacy Protection Rule, all the following would be considered personal information EXCEPT:

    A. The children's first and last names
    B. Gamer Tags or other User IDs
    C. Identifying favorite shows on streaming services
    D. Any picture showing the child's face

12. Which statement is **TRUE** regarding Sarah and Robert under COPPA?

    A. COPPA applies to both Sarah and Robert
    B. COPPA applies to Sarah, but not Robert
    C. COPPA applies to Robert, but not Sarah
    D. COPPA applies to neither Robert nor Sarah

13. One of Don's concerns is the easy access to pornography on the internet today. He does not want his children viewing pornography either purposely or accidentally. Which statement is TRUE regarding protecting children from pornography?

    A. COPPA will prevent a child from lying about their age to view adult content.
    B. COPPA will prevent web sites from displaying pornography to children.
    C. Don can prevent his children from watching pornography by controlling what apps they install.
    D. Don can discourage his children from viewing pornography by understanding and using parental controls on all their devices.

14. Don understands that some location-based services simply enhance the user experience. Others, such as daily fantasy sports applications that allow sports betting, require that location-based services be activated to function at all. Given Don's concern over his children's safety, which of the following best practices would you recommend to Don?

    A. Do not allow the children to use location-based services at all.
    B. Allow the children to turn on location-based services on their smart phones, but not their gaming consoles.
    C. Allow the children to turn on location-based services on their gaming consoles, but not their smart phones.
    D. Allow the children to turn on location-based services on all their devices.

15. Robert has been having some arguments with another boy at school. The other boy has posted a picture semi-nude picture of Robert on social media that he took in the boy's locker room after football practice. Along with the picture the boy identified Robert by first and last name and what school they attend. Regarding privacy law, what course of action would you recommend to Don in this situation?

A. Contact the social media website to have the content removed.
B. Report the incident to the FTC since they have specific authority for COPPA.
C. Have Robert do the same thing to the other boy.
D. Attempt to contact the boy's parents and make them remove the picture and information.

---

16. Which of the following requires financial institutions to maintain security controls to protect personal consumer information for both electronic and paper records, and requires institutions to implement an information security program?

A. California Financial Information Privacy Act
B. Privacy Rule
C. Red Flags Rule
D. Safeguard Rule

17. General health records data for private schools who accept no federal funding are subject to:

A. FERPA
B. PPRA
C. HIPAA
D. No Child Left Behind

18. The criteria for an existing business relationship, as defined by TSR, includes:

A. A transaction taking place within the last 18 months.
B. A transaction taking place within the past two years.
C. An offer has been requested within the past year.
D. An offer has been requested within the last six months.

19. Who has the right to private action regarding violations of the CAN-SPAM Act?

A. Businesses who receive unsolicited advertisements to business email addresses.
B. Governmental agencies who receive unsolicited advertisements to .gov addresses.
C. Individuals who receive unsolicited advertisements to personal email addresses.
D. Internet Service Providers attempting to protect their customers from unsolicited email advertisements.

Use the following scenario to answer questions 20-24.

Lawrence works in the billing office of TH Medical Clinic. Lawrence is 30 years old with a bachelor's degree in finance. Lawrence received training during his orientation that included what PHI is collected, when it is collected, how it is stored, when it is destroyed, when it is updated, and an overview of HIPAA requirements as they related to his position.

Since he is in billing, Lawrence has the highest security classification in at the medical clinic since he sees PHI for the patient, payment information for the patient, insurance information, and billing codes related to each patient's diagnosis and treatment at the clinic. Lawrence has been asked to be a trainer in the future for new employees who will need to understand HIPAA and various processes in the company related to the data. Therefore, Lawrence is reviewing his own materials to refresh his memory.

20. What was the primary reason for the creation of HIPAA?

A. To introduce protected health information security measures.
B. To increase the efficiency of electronic healthcare payments.
C. To create a common database within healthcare systems for patient diagnosis and prescription management.
D. To extend privacy laws to business associates within health care.

21. Lawrence works for a healthcare provider, which of the following healthcare entities covered by HIPAA (prior to HITECH) includes third-party organizations that host, handle, or process medical information?

A. Business Associates
B. Healthcare Clearinghouses
C. Healthcare Plans
D. Healthcare Controllers

22. Which of the following scenarios would NOT be covered under HIPAA?

A. Doctor visit for annual physical
B. Chemotherapy related to cancer treatment in a medical facility
C. Billing codes, patient name, and insurance identification sent to an insurance company for payment
D. Medical books purchased through Amazon

23. What is the primary purpose of the HIPAA Security Rule?

A. Establish minimum security requirement for medical facilities following the 2001 terrorist attacks.
B. Establish minimum security requirements for PHI collected in any form.
C. Establish minimum security requirements for PHI collected in electronic form.
D. Establish a secure manner of payment processing for insurance claims.

24. All the following are security requirements set forth by the HIPPA Security Rule, except:

A. Designate a responsible person for the security program.
B. Ensure compliance by the workforce and implement a security and awareness training program.
C. Conduct initial and ongoing risk assessments.
D. Establish an annual compliance audit process with the Office of Civil Rights.

25. Which of the following is not a legal requirement when a potential employer is using information in a consumer report to determine employment eligibility?

A. A permissible purpose must exist for the report information.
B. The candidate must receive written notice that a report will be requested.
C. The candidate must give written consent before the report is obtained.
D. The candidate must receive notice whether adverse action was taken or not.

26. Under Section 702 of FISA, which surveillance program allows data requests of Internet Service Providers?

A. PRISM
B. MAGENTA
C. RAINBOW
D. Upstream

27. In which of the following laws is disclosure forbidden unless a person has expressly opted-in?

A. Bank Secrecy Act
B. COPPA
C. GLBA
D. US Patriot Act

28. Based on current US employment privacy laws, which of the following should NOT be expected to happen while employed with a company?

A. Taking a polygraph test due to a theft at work.
B. Video monitoring only for workplace safety compliance.
C. GPS tracking while making deliveries for work.
D. A manager accessing your computer to get an needed file while you are on vacation.

29. "Third party doctrine" as it relates to the fourth amendment of the US constitution concerns:

A. Three authorities are required for creating and administering a warrant.
B. Someone referring to themselves in the third person is hiding something.
C. Data or information a suspect shares with a third party is not privacy protected.
D. A third party can wiretap a suspect without a warrant and then give the data to the police.

30. Which legislation provides protection to the media from government searches unless they have committed a crime or threaten to commit a crime?

A. US Communications Assistance to Law Enforcement
B. Stored Communications Act
C. Privacy Protection Act
D. Cybersecurity Information Sharing Act

References

1. Answer: A. The essential definition of privacy is the right to be let alone. It also has been defined as “the desire of people to freely choose the circumstances and the degree to which individuals will expose their attitudes and behaviors to others.”

2. Answer: C. A consent decree can be imposed for up to 20 years.

3. Answer: B. The new program should be communicated to internal (privacy policy) and external (privacy notice) audiences. Transparency is key.

4. Answer: B. In general, sensitive data must have a higher classification level and should be better protected. The number of employees who have access is then limited based on the classification level. Data classification is often mandatory in the US based on sectoral legislation. It also has advantages: it helps to comply with compliance audits, helps to quickly comply with legal (discovery) requests and storage capacity is used efficiently.

5. Answer: D. The GPDR applies to companies with assets and employees in the EU, to companies that sell to people in the EU and to data processed in the EU.

6. Answer: A. Phishing; users are encouraged by emails or other expressions to share usernames and passwords with parties who act as a legitimate party such as a bank, but who misuse the data obtained. Spear phishing: is phishing aimed at an individual user.

7. Answer B: The Office of Civil Rights (OCR) is the primary enforcer of the HIPAA Privacy Rule. The U.S. Department of Justice (DOJ) has criminal enforcement authority. The FTC and state attorneys general can bring enforcement for unfair and deceptive practices.

8. Answer: A. The purpose of the 21st Century Cures Act (“Cures Act”) is to expedite the research process for new medical devices and prescription drugs, quicken the process for drug approval, and reform mental health treatment.

9. Answer: B. Under the FCRA users must notify consumers when third-party (CRA) data is used to make adverse decisions about them.

10. Answer: A. FACTA has introduced measures for identity theft protection, together with a Disposal Rule and a Red Flags Rule.

11. Answer C. Identifying favorite shows or selecting viewing preference such as genre would not be personal information since it cannot identify the person.

12. Answer B. COPPA applies to children under the age of 13.

13. Answer D. The best way to prevent children from viewing porn is to talk with the children about what is allowable and what is harmful and using parental controls to block adult websites along with steaming content and games based on their ratings.

14. Answer C. Location-based services often just need to know the general area someone is in such as the state they are in now, and not their specific address. However, most mobile devices, like smart phones, are only used by a single individual. This complicates things because when that individual carries their mobile device everywhere with the location-based services turn on the identity of the person can be inferred based on their location, such as Sarah going to her middle school each day. Since she is the only person in the family that attends the school each day, one could infer that she owns the device. Don should not allow location-based services on the smart phone, or only allow location-based services to be activated when the children are home from school, or on the weekends.

15. Answer A. COPPA does not cover minors between that age of 13 and 18. However, California's Privacy Rights for California Minors in the Digital World allows Robert and his family to contact the social media website to have the content removed.

16. Answer: D. The Safeguards Rule (2003) requires financial institutions to maintain security controls to protect personal consumer information. The rule applies to electronic and paper records. Institutions must implement an information security program.

17. Answer: C. If a school is not subject to FERPA, such as private schools, then the medical records of this school (if a covered entity) are subject to the HIPAA Privacy Rule.

18. Answer: A. an existing business relationship exists when a transaction has taken place in the last 18 months or an offer has been requested in the last 3 months.

19. Answer: D. Internet service providers have a right to private action (other parties do not).

20. Answer: B. Although HIPAA contains extensive privacy protection, the law is mainly adopted to increase the efficiency of (electronic) healthcare payments.

21. Answer: B. Healthcare Clearinghouses are third-party organizations that host, handle, or process medical information. These are HIPAA covered entities now.

22. Answer: D. It is important to understand that HIPAA applies to these covered entities, but not to other healthcare providers and services. Individuals surfing the web or purchasing books about healthcare are not covered by HIPAA.

23. Answer: C. The Security Rule establishes minimum security requirements for PHI that a covered entity receives, creates, maintains, or transmits in electronic form.

24. Answer: D. Formalized annual audits with OCR are not established.

25. Answer: D. Candidates must only receive notice for any adverse actions.

26. Answer: A. Two surveillance programs are currently authorized under Section 702: PRISM and Upstream. With PRISM, data requests can be made to ISPs. Upstream is about searching internet-based communications as they pass through physical U.S. internet infrastructure.

27. Answer: B. Disclosure of information is prohibited in many laws. An opt-in to disclose information may be required (HIPAA, COPPA). In some cases, an opt-out (GLBA) applies.

28. Answer: A. Under the Employee Polygraph Protection Act of 1988 (EPPA), employers are not allowed to use "lie detectors" on workers or candidates.

29. Answer: C. The Supreme Court has confirmed that information placed in the hands of a "third party" is not protected by the Fourth Amendment. For example, no warrant is required to request a list of called persons. This third-party doctrine means that companies may provide data from employees or customers to the government.

30. Answer: C. The Privacy Protection Act (PPA) of 1980 protects the media against house searches. An exception applies if the person or organization in question has committed a crime itself or threatens to commit a crime. Having such information does not count as such a crime.