

IAPP Information Privacy Certification

CIPP Practice Examination



The Certified Information Privacy Professional (CIPP) examination is a timed, two-hour, objective test that is evenly divided into five subject matter areas: (1) Privacy Law and Compliance; (2) Workplace Privacy; (3) Information Security; (4) Web Privacy and Security; and, (5). Data Sharing and Transfer. Each section contains 25 multiple choice items plus one case study with ten true/false items pertaining to that case study. One exam section is equivalent to 35 total points (1 point per item). A minimum score of 123 total points (70%) is required for an individual to pass the entire CIPP examination and become certified by IAPP.

The following sample exam questions draw from all five subject matter areas in the CIPP curriculum. They illustrate the structure, format, and level of difficulty that you can expect to find in the actual CIPP examination. An answer key is provided on page 9.

For purposes of self-testing, you may set the timing requirement at 24 minutes for the 35 items listed. This is the equivalent of a single section on the actual CIPP examination.

1. The Children's Online Privacy Protection Act (COPPA):

- A. Prohibits any collection of personal information about children under the age of 13
- B. Enables the Federal Trade Commission (FTC) to regulate marketing to children
- C. Is an attempt to regulate children's online access to pornography
- D. Restricts the online collection of personal information from children under the age of 13 and without parental consent

2. The California data breach notification law (SB 1386):

- A. Defines personal information as the person's name only
- B. Does not provide for monetary damages in the event of a breach
- C. Is enforced by the California Attorney General and allows for a private right of action
- D. Requires encryption of all personal information

- 3. Which of the following is not a generally required action for a health care provider under the Health Insurance Portability and Accountability Act (HIPAA)?**
 - A. Notify patients about their privacy rights and how their information can be used
 - B. Train employees so that they understand the privacy procedures
 - C. Designate an individual responsible for seeing that the privacy procedures are adopted and followed
 - D. Provide an opportunity to opt out of sharing protected health information with non-affiliated third parties for the third parties' own marketing activities

- 4. Under the Fair Credit Reporting Act (FCRA), an organization that uses a consumer report is required to:**
 - A. Ensure that data for substantive decision-making must be appropriately accurate, current and complete
 - B. Provide notice to consumers when a report's data is used to make adverse decisions about them
 - C. Allow consumers to have access to their consumer reports and an opportunity to dispute and correct errors
 - D. All of the above

- 5. Model contracts are used to:**
 - A. Ensure legal compliance with E.U. data protection laws
 - B. Any time PII is to be exchanged
 - C. Determine if employee data is involved
 - D. Comply with U.S. government agency standards

- 6. "Social engineering" is the technique by which:**
 - A. Information security managers establish controls that protect the integrity of sensitive or personal data within an organization
 - B. Policy makers formulate procedural guidelines for the use, sharing or disclosure of sensitive or personal data within a community
 - C. Hackers or exploit artists use psychological persuasion or coercion in order to gain access to sensitive or personal data
 - D. Scientists and academics determine public attitudes concerning the handling of sensitive or personal data by governments, businesses and other organizations

- 7. A privacy impact assessment (PIA) process helps:**
 - A. Evaluate the strengths of your existing privacy program
 - B. Determine the risks associated with a new operation
 - C. Only if you are working on a U.S. government contract
 - D. Only if you are building a new Website

- 8. Which one of the following categories defines data elements that are considered non-public personal information under the Gramm-Leach-Bliley Act?**
 - A. A consumer's full name
 - B. A consumer's home mailing address
 - C. A consumer's home telephone number
 - D. A consumer's home email address

- 9. HIPAA covered entities must provide privacy and security training to:**
 - A. All employees
 - B. Only employees that come into contact with PHI
 - C. Business associates that process PHI
 - D. HIPAA covered entities are not required to provide privacy and security training

- 10. Which one of the following sources of personal information are U.S. employers permitted to access when conducting a background screening of prospective new hires?**
 - A. Military discharge records.
 - B. Arrest records.
 - C. Credit reports with the person's written consent.
 - D. None of the above.

- 11. Under what circumstances is it permissible to monitor employees in the workplace?**
- A. In order to prevent a crime or act of violence in the workplace
 - B. In order to control the quality of products or services
 - C. In order to reduce absenteeism
 - D. All of the above are permissible reasons to monitor employees in the workplace
- 12. Soleil is a chain of exercise clubs and resorts. The company offers excellent health benefits to its employees. These include complete medical, dental, prescription and eye care benefits. Which single statement below is true regarding Soleil's privacy obligations?**
- A. Soleil is obligated to protect employee benefit information in accordance with its privacy policy only
 - B. Soleil is obligated to protect employee benefit information in accordance with HIPAA requirements for covered entities
 - C. Soleil is obligated to protect employee benefit information in accordance with HIPAA requirements for business associates
 - D. Soleil is not obligated to protect employee benefit information under U.S. law but as a general rule it needs to keep all medical records as strictly confidential
- 13. Which laws govern employee rights in the United States?**
- A. The U.S. federal government has specific regulations about protecting employee privacy
 - B. Most state governments have specific regulations about protecting employee privacy
 - C. Common laws in the United States provide employees with specific legal remedies
 - D. Civil rights provide employees with specific remedies
- 14. Which of the following statements is false regarding U.S. employee privacy policies generally?**
- A. Most organizations are required by law to have an employee privacy policy
 - B. Employees have a right to view all information contained in employment records at all times
 - C. Most organizations are required to keep a record that verifies employment status indefinitely
 - D. All of the above are false statements

15. Sanctions and fines were imposed by the FTC on the following company for failure to evidence appropriate privacy training to employees:

- A. Wells Fargo
- B. Guess Jeans
- C. Eli Lilly
- D. Amazon.com

16. Authentication is:

- A. The process by which a user provides a password in order to gain access to protected information
- B. The process by which a person or a computer system determines that another entity actually is who/what it claims to be
- C. The process by which a user is granted access rights and permissions to protected information
- D. The process by which a user is assigned security clearance to protected information

17. Which one of the following best describes the process of "two-factor" authentication?

- A. An associate enters his or her user ID and password to access a protected resource.
- B. An associate enters his or her user ID, password and social security number/social identification number in order to access a protected resource.
- C. An associate enters his or her user ID, password, and swipes his or her smart card to access a protected resource.
- D. An associate swipes his or her badge to access a protected resource.

18. Which one of the following is not used in biometric systems to authenticate individuals?

- A. Password
- B. Fingerprinting
- C. Voice recognition
- D. Iris scan

19. The best way to ensure compliance with privacy standards in IT development is:

- A. Sending memoranda to the IT group
- B. Creating a privacy requirements document for the IT group
- C. Ensuring that internal audit knows how to audit for privacy concerns
- D. All of the above

20. An/a _____ is a private data network that outside partners can access.

- A. Intranet
- B. Local Area Network (LAN)
- C. Extranet
- D. Web portal

21. While browsing an automotive Website, you are served a banner advertisement for sporting and hiking equipment. This ad is most likely to have been delivered by which one of the following Web technologies:

- A. A Web beacon
- B. A persistent third-party cookie
- C. A persistent first-party cookie
- D. A pixel tag

22. Which one of the following statements is true regarding the emerging online threat of “phishing”?

- A. Phishing begins most often with a telephone call
- B. Phishing occurs when an Internet user is lured to a fraudulent Website
- C. Phishing is a violation of the CAN-SPAM Act
- D. Phishing is also known as spoofing

23. What types of PII are exempt from trans-border data regulations?

- A. Medical history
- B. Credit history
- C. Social Security Numbers
- D. Personnel records

24. Which one of the following statements is true about the sharing of demographic databases if there is no information that can be used to identify a particular person?

- A. European companies can freely develop and share demographic databases with U.S. companies
- B. U.S. companies must obtain consent from the European data subject before being able to obtain information from European companies
- C. U.S. companies must obtain consent from the appropriate European data protection authority before being able to obtain information from European companies
- D. Only U.S. companies in compliance with Safe Harbor can freely obtain demographic databases from European companies

25. The OECD guidelines:

- A. Have become the foundation of most data protection laws around the world today
- B. Were replaced by the Council of Europe's COE Convention of 1981
- C. Set forth basic privacy principles as agreed by a 23-nation body that includes Europe and Japan but not the United States
- D. Did not receive the approval of the Federal Trade Commission (FTC)

26. Information Privacy Case Study

Jim is a systems engineer for Productis, a major U.S. consumer goods company and his job requires him to spend many hours on planes traveling to and from the company's far-flung locations and plants. During such trips, Jim relies on his office laptop computer to connect to the company's network and communicate with his employees.

Jim's teenage son, Randy, felt sorry about his father's travel schedule and wanted to do something entertaining to help relieve the stress.

One weekend, Randy downloaded a multimedia game player onto his father's office laptop computer. However, neither Randy nor Jim realized at the time that the "free" multimedia player Randy downloaded came bundled with another software application—a "spyware" program—that captured information regarding Jim's network connection, IP address and system log-on.

Please indicate whether each statement below is TRUE or FALSE by writing your selection in the space provided.

- 1. Jim should not remove the multimedia player without the aid of an expert because the act of removal can damage Jim's laptop settings.
- 2. As a general rule, the company's policy should expressly state that only Jim should have custody of his company laptop.
- 3. Most companies have embedded controls that prevent the downloading of all non-approved software applications.
- 4. Jim should have contacted the technical support department in his company and immediately stopped using his computer once he realized that unauthorized software was downloaded.
- 5. As a general rule, Jim would not cause a serious privacy or security breach if he used his laptop with unauthorized software as long as it didn't connect to his company's mainframe or network.
- 6. The act of downloading the spyware program, without Jim's consent, is a violation of U.S. federal law.
- 7. The act of downloading the spyware program without Jim's consent always creates legal liability for multimedia software company.
- 8. The act of downloading the spyware program without Jim's knowledge is always a violation of law.
- 9. One of the most important controls to prevent problems with unauthorized downloads and spyware is to educate employees about the risk.
- 10. Because of increased risks associated with spyware, it is a good idea to expressly include "dos and don'ts" about unauthorized downloads in the company's security policy or standard operating procedures.

Answer Key

Multiple Choice Questions	Case Study True/False
1. D 2. C 3. D 4. D 5. A 6. C 7. B 8. D 9. A 10. C 11. D 12. A 13. C 14. B 15. C 16. B 17. C 18. A 19. D 20. C 21. B 22. B 23. C 24. A 25. A	1. T 2. T 3. F 4. T 5. F 6. F 7. F 8. F 9. T 10. T