

Certified in Healthcare Privacy and Security (CHPS) Examination

Content Outline

Number of Questions on Exam:

Exam Time: 4 hours

DOMAIN I. Ethical, Legal, and Regulatory Issues/External Environmental Assessment (22%)

TASKS.

1. Serve as a resource (provide guidance) to your organization regarding privacy and security laws, regulations, and standards of accreditation agencies to help interpret and apply the standards.
2. Develop incident response plan and identify team members (e.g. Human Resources, Legal, Risk Management, Physical Security, Law Enforcement, Public Relations, IT, Administration) to respond to a privacy or security incident.
3. Demonstrate privacy and security compliance with documentation, production and retention as required by State and Federal law as well as accrediting agencies

DOMAIN II. Program Management and Administration (22%)

TASKS.

1. Administer an appropriate organizational infrastructure for privacy and information security to oversee the program(s).
2. Create, document, and communicate information privacy and security policies, procedures, consents, authorizations, notice of privacy practices.
3. Identify contracts and business relationships and secure appropriate agreements related to privacy and security (e.g., BAA, QSO, etc.). Manage business associate relationships throughout the life of the contract.
4. Evaluate and monitor facility security plan to safeguard unauthorized physical access to information and prevent theft or tampering.
5. Develop, deliver, evaluate and document training and awareness on information privacy and security to provide an informed workforce.
6. Work with appropriate organization officials to verify that information used or disclosed for research complies with organizational policies and procedures and applicable privacy regulations.
7. Assess, recommend, revise, and communicate changes to organizational policies, procedures, and practices related to privacy and security.
8. Assess and communicate risks and ramifications of privacy and security incidents, including those by business associates.
9. Establish a preventative program to detect, prevent and mitigate privacy/security breaches.
10. Apply and recommend appropriate de-identification methodologies
11. Verify that requesters of protected information are authorized and permitted to receive the protected information (subpoena, court orders, search warrants)
12. Define HIPAA-designated record sets for the organization in order to appropriately respond to a request for release of information.
13. Identify information and record sets requiring special privacy protections.

14. Serve as a resource (provide guidance) to your organization regarding privacy and security laws, regulations, and standards of accreditation agencies to help interpret and apply the standards.
15. Develop minimum necessary procedures.
16. Recommend, review and approve protocols to verify identity and access rights of recipients/users of health information.

DOMAIN III. Information Technology/Physical and Technical Safeguards (18%)

TASKS.

1. Facilitate development and verify maintenance of the inventory of software, hardware, and all information assets to protect information assets and to facilitate risk assessment.
2. Participate in business continuity planning for planned downtime and contingency planning for emergencies and disaster recovery.
3. Participate in evaluation, selection, and implementation of information privacy and security solutions.
4. Develop a systematic process to evaluate risk to and criticalities of information systems which contain PHI.
5. Assess, implement and oversee media control practices that govern the receipt, removal, re-use, or disposal (internal and external destruction) of any media or devices containing sensitive data to protect the confidentiality, privacy and security of information.
6. Assess and monitor physical security mechanisms to limit the access of unauthorized personnel to facilities, equipment and information.
7. Establish reasonable safeguards to reduce incidental disclosures
8. Participate in the development and management of the organization's information security plan.
9. Participate in the organizational risk assessment plan to identify threats and vulnerabilities.
10. Monitor compliance with the security policies.
11. Ensure adequacy of technical safeguards such as configuration management, intrusion detection, and preventive countermeasures.
12. Establish internal policies, procedures and rules to protect information and comply with security requirements.
13. Apply appropriate technologies to protect information received from or transmitted to external users (HIEs, RHIOs, PHRs, and other third parties).
14. Verify and validate data backup plan.
15. Participate in development of guidelines, procedures and controls to ensure the integrity, availability and confidentiality of communication across networks (e.g. wireless, Internet, secure sockets, VPNs, and PKI).
16. Advocate the use of event triggering to identify abnormal conditions within a system (e.g. intrusion detection, denial of service, and invalid log-on attempts).
17. Establish and manage process for verifying and controlling access authorizations and privileges including emergency access
18. Establish and manage authentication mechanisms.
19. Recommend use of encryption of protected health information and other sensitive data based on risk assessment.

DOMAIN IV. Investigation, Compliance, and Enforcement (23%)

TASKS.

1. Monitor and assess compliance with state and federal laws and regulations related to privacy and security to update organizational practices, policies, procedures and training of staff members.
2. Coordinate the organization's response to inquiries and investigations from external entities relating to privacy and security to provide response consistent with organizational policies and procedures.
3. Develop performance measures and reports to monitor and improve organizational performance and report to appropriate organizational body.
4. Enforce privacy and security policies, procedures, and guidelines to facilitate compliance with federal, state, and other regulatory or accrediting bodies.
5. Monitor access to protected health information.
6. Establish an incident/complaint investigation response and resolution process for privacy and security incidents.

DOMAIN V. Customer/Client/Patient Services (15%)

TASKS.

1. Establish, maintain, and distribute the organization's Notice of Privacy Practices.
2. Inform the individual who is the subject of individually identifiable health information of their information privacy rights related to the use and disclosure of protected information
3. Establish and maintain an operational system to receive, process, and document requests for:
 - Amendments
 - Access to PHI
 - Accounting of disclosures
 - Alternate means of communication
 - Restrictions
 - Complaints
4. Develop and implement communication tools, as appropriate for the organization, to keep individuals informed on the organization's commitment to information privacy and security, their individual rights, and services based on their individual rights.
5. Breach notification (federal):
 - Develop policy and procedure
 - Educate workforce on reporting requirements
 - Develop risk assessment tools
 - Notify appropriate individuals/agencies/media within time frame
 - Maintain the appropriate documentation