Certified in Healthcare Privacy and Security (CHPS) Examination Content Outline

Number of Questions on Exam:

- **150 multiple-choice (125 scored/25 pretest)**

Exam Time: 3.5 hours – no breaks

Domain 1 – Ethical, Legal, and Regulatory Issues/ Environmental Assessment (23-27%)

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. Demonstrate privacy and security compliance with documentation, production and retention as required by State and Federal law as well as accrediting agencies
3. Identify responsibilities as a privacy officer and/or security officer

Domain 2 – Program Management and Administration (23-27%)

Tasks:

1. Create, document, and communicate information to include but not limited to minimum necessary protocols
2. Manage contracts and business associate relationships and secure appropriate agreements related to privacy and security (e.g., BAA, SLA, etc.)
3. Evaluate and monitor facility security plan to safeguard unauthorized physical access to information and prevent theft or tampering
4. Develop, deliver, evaluate and document training and awareness on information privacy and security to provide an informed workforce
5. Work with appropriate organization officials to verify that information used or disclosed for research complies with organizational policies and procedures and applicable privacy regulations
6. Assess, recommend, revise, and communicate changes to organizational policies, procedures, and practices related to privacy and security
7. Assess and communicate risks and ramifications of privacy and security incidents, including those by business associates
8. Establish a preventative program to detect, prevent and mitigate privacy/security breaches
9. Recommend appropriate de-identification methodologies
10. Verify that requesters of protected information are authorized and permitted to receive the protected information (subpoena, court orders, search warrants)
11. Define HIPAA-designated record sets for the organization in order to appropriately respond to a request for release of information
12. Identify information and record sets requiring special privacy protections
13. Recommend, review and approve protocols to verify identity and access rights of recipients/users of health information
14. Establish, maintain, and ensure the distribution process of the organization's Notice of Privacy Practices

15. Establish and maintain operational systems to receive, process, and document requests for patients' rights as outlined in the Notice of Privacy Practices

Domain 3 – Information Technology/Physical and Technical Safeguards (23-27%)

Tasks:

1. Participate in the development and verify maintenance of the inventory of software, hardware, and all information assets to protect information assets and to facilitate risk analysis
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. Implement a systematic process to evaluate risk to and criticalities of information systems which contain PHI
5. Participate in media control practices that govern the receipt, removal, re-use, or disposal (internal and external destruction) of any media or devices containing sensitive data
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 and prevent privacy breaches
8. Participate in the development and management of the organization's information security plan
9. Participate in the organizational risk analysis plan to identify threats and vulnerabilities
10. Monitor compliance with the security policies and ensure compliance with technical, physical, and administrative safeguards
11. Establish internal policies, procedures and rules to protect information and participate in development of guidelines, procedures and controls to ensure the integrity, availability and confidentiality of communication across networks
12. Ensure appropriate technologies are used to protect information received from or transmitted to external users
13. 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).
14. Establish and manage facilitate process for verifying and controlling access authorizations, authentication mechanisms, and privileges including emergency access
15. Evaluate the use of encryption for protected health information and other sensitive data

Domain 4 – Investigation, Compliance, and Enforcement (23-27%)

Tasks:

1. Monitor assess compliance with state and federal laws and regulations related to privacy and security to update organizational practices, policies, procedures and training of workforce
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, develop response plan, and identify team members to respond to a privacy or security incident

7. Coordinate mitigation efforts
8. Develop policy and procedure for breach notification (federal)
9. Educate workforce on reporting requirements for breach notification (federal)
10. Perform risk assessment for breach notification (federal)
11. Notify appropriate individuals/agencies/media within time frame for breach notification (federal)
12. Maintain the appropriate documentation for breach notification (federal)