

Domain 1 – Ethical, Legal, and Regulatory Issues/ Environmental Assessment (10-18%)

Tasks:

1. Identify responsibilities as a privacy officer and/or security officer
2. 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
3. Apply preemption principles to ensure compliance with state regulations that are applicable to privacy
4. Evaluate the privacy and security policies related to health information exchanges
5. Demonstrate privacy and security compliance with documentation, production and retention as required by State and Federal law as well as accrediting agencies
6. Analyze the impact of access to protected health information (PHI) during a public health emergency

Domain 2 – Privacy and Security Program Management and Administration (30-40%)

Tasks:

1. Manage the distribution process of the organization's Notice of Privacy Practices
2. Manage the process for requests for patients' rights as outlined in the Notice of Privacy Practices (e.g., restrictions, amendments, etc.)
3. Manage contracts and business associate relationships and secure appropriate agreements related to privacy and security (e.g., business associate agreement [BAA], service level agreement [SLA], etc.)
4. Evaluate and monitor the facility security plan to safeguard unauthorized physical access to information, and to prevent theft or tampering
5. Establish a preventative program to detect and prevent privacy/security breaches
6. Develop, deliver, evaluate, and document training and awareness on information privacy and security to provide an informed workforce
7. Educate workforce members on the changes to organizational policies, procedures, and practices related to privacy and security
8. Collaborate with appropriate organization officials to verify that information used or disclosed for research purposes complies with organizational policies and procedures and applicable privacy regulations
9. Manage appropriate de-identification processes
10. Assess and communicate risks and ramifications of privacy and security incidents to a designated organizational leadership, including those by business associates
11. Verify that requesters of protected information are authorized and permitted access to the protected health information (PHI)
12. Apply the "minimum necessary" standard when creating, documenting, and communicating protected health information (PHI)
13. Define HIPAA-designated record sets for the organization in order to appropriately respond to a request for release of protected health information (PHI)
14. Identify information and record sets requiring special privacy protections

15. Manage disclosures for marketing and fundraising related to protected health information (PHI)

Domain 3 – Information Technology/Physical and Technical Safeguards (24-35%)

Tasks:

1. Develop and manage an organization's information security plan, taking into consideration 45 CFR 164.306
2. Manage policies, procedures, and rules to protect the integrity, availability, and confidentiality of communication of health information across networks
3. Ensure reasonable safeguards to reduce incidental disclosures and prevent privacy breaches
4. Collaborate in the development of a business continuity plan for planned downtime and contingency planning for emergencies and disaster recovery
5. Evaluate, select, and implement information privacy and security solutions
6. Monitor compliance with the security policies and ensure compliance with technical, physical, and administrative safeguards
7. Assess the risk to and criticalities of new information systems which contain protected health information (PHI)
8. Assess and monitor physical security mechanisms to limit the access of unauthorized personnel to facilities, equipment, and information
9. Assess and monitor technical security mechanisms to control access and protect electronic protected health information (PHI)
10. Perform ongoing risk assessments for existing information systems which contain protected health information (PHI)
11. Ensure appropriate technologies are used to protect information received from or transmitted to external users
12. Manage the process for verifying and controlling access authorizations, authentication mechanisms, and privileges including emergency access
13. Identify event triggers for abnormal conditions within a network system (e.g., intrusion detection, denial of service, and invalid log-on attempts)
14. Manage the media control practices that govern the receipt, removal, re-use, or disposal (internal and external destruction) of any media or devices containing sensitive data
15. Develop and maintain the inventory of software, hardware, and all data to protect information assets and to facilitate risk analysis

Domain 4 – Investigation, Compliance, and Enforcement (19-24%)

Tasks:

1. Monitor and assess compliance with state and federal laws and regulations on a routine basis related to privacy and security to update organizational practices, policies, procedures, and training of workforce
2. Develop policy and procedure for breach notification
3. Establish an incident/complaint investigation process, and develop a response plan to mitigate a privacy or security incident
4. Ensure workforce is knowledgeable on how to report a potential privacy or security incident
5. Enforce privacy and security policies, procedures, and guidelines to facilitate compliance with federal, state, and other regulatory or accrediting bodies
6. Monitor and audit access to protected health information (PHI)

7. Perform risk assessment for breach notification
8. 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 within the required timeframe
9. Notify appropriate individuals/agencies/media within time frame for breach notification
10. Maintain the appropriate documentation for breach notification