HHS Office for Civil Rights

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html [Accessed on January 18, 2013]

Audit Program Protocol:

The OCR HIPAA Audit program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits. The entire audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. The combination of these multiple requirements may vary based on the type of covered entity selected for review.

- The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.
- The protocol covers Security Rule requirements for administrative, physical, and technical safeguards
- The protocol covers requirements for the Breach Notification Rule.

The protocol is available for public review and searchable by keyword(s) in the table below.

HIPAA Security Rule

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
§164.308	§164.308(a)(1): **Security Management Process §164.308(a)(1)(ii)(a)** - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Conduct Risk Assessment	Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Obtain and review relevant documentation and evaluate the content relative to the specified criteria for an assessment of potential risks and vulnerabilities of ePHI. Evidence of covered entity risk assessment process or methodology considers the elements in the criteria and has been updated or maintained to reflect changes in the covered entity's environment. Determine if the covered entity risk assessment has been conducted on a periodic basis. Determine if the covered entity has identified all systems that contain, process, or transmit ePHI.	Required
§164.308	§164.308(a)(1)(i): **Security Management Process** - Although the HIPAA Security Rule does not require purchasing any particular technology, additional hardware, software, or services may be needed to adequately protect information. Considerations for their selection should include the following: -Applicability of the IT solutions to the intended environment; -The sensitivity of the data; -The organization's security policies, procedures, and standards; and -Other requirements such as resources available for operation, maintenance, and training.	Acquire IT Systems and Services	Inquire of management as to whether formal or informal policy and procedures exist covering the specific features of the HIPAA Security Rule information systems §164.306(a) and (b). Obtain and review formal or informal policy and procedures and evaluate the content in relation to the specified performance to meet the HIPAA Security Rule §164.306(a) and (b). Determine if the covered entity's formal or informal policy and procedures have been approved and updated on a periodic basis.	Required
§164.308	§164.308(a)(1)(ii)(D): **Security Management Process** - Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Develop and Deploy the Information System Activity Review Process	Inquire of management as to whether formal or informal policy and procedures exist to review information system activities; such as audit logs, access reports, and security incident tracking reports. Obtain and review formal or informal policy and procedures and evaluate the content in relation to specified performance criteria to determine if an appropriate review process is in place of information system activities. Obtain evidence for a sample of instances showing implementation of covered entity review practices Determine if the covered entity policy and procedures have been approved and updated on	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
			a periodic basis.	
§164.308	§164.308(a)(1): **Security Management Process §164.308(a)(1)(ii)(b)** - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Implement a Risk Management Program	Inquire of management as to whether current security measures are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). Obtain and review security policies and evaluate the content relative to the specified criteria. Determine if the security policy has been approved and updated on a periodic basis. Determine if security standards address data moved within the organization and data sent out of the organization.	Required
§164.308	§164.308(a)(2): **Assigned Security Responsibility** - the responsibility for security should be assigned to a specific individual or organization to provide an organization focus and importance to security, and that the assignment be documented.	Select a Security Official To Be Assigned Responsibility for HIPAA Security	Inquire of management as to whether the organization has assigned responsibility for the HIPAA security to a Security Official to oversee the development, implementation, monitoring, and communication of security policies and procedures. Obtain and review the assigned Security Official's responsibilities (e.g., job description) and evaluate the content in relation to the specified criteria. Determine if the responsibilities of Security Official have been clearly defined.	Required
§164.308	§164.308(a)(2): **Assigned Security Responsibility** - the responsibility for security should be assigned to a specific individual or organization to provide an organization focus and importance to security, and that the assignment be documented.	Assign and Document the Individual's Responsibility	Inquire of management as to whether the roles and responsibilities of the assigned individual or organization are properly documented in a job description and communicated to the entire organization. Obtain and review the Security Official's job description and evaluate the content in relation to the specified criteria. Determine that the roles and responsibilities of the Security Official have been clearly identified in a job description.	Required
§164.308	§164.308(a)(3)(ii)(A): **Workforce security** - Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Implement Procedures for Authorization and/or Supervision	Inquire of management as to whether the level of authorization and/or supervision of workforce members has been established. Obtain and review the entity's organizational chart or other formal documentation and evaluate the content in relation to the specified criteria to determine the existence of chains of command and lines of authority. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.308	§164.308(a)(3): **Workforce Security** - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this	Establish Clear Job Description and Responsibilities	Inquire of management as to whether the roles and responsibilities of the assigned individual or organization are properly documented in a job description and communicated to the entire organization. Obtain and review the Security Official's job description and evaluate the content in relation to the specified criteria. Determine that the roles and responsibilities of the Security Official have been clearly identified in a job	Addressable

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.		description.	
§164.308	§164.308(a)(3): **Workforce Security** - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Establish Criteria and Procedures for Hiring and Assigning Tasks	Inquire of management as to whether staff members have the necessary knowledge, skills, and abilities to fulfill particular roles. Obtain and review formal documentation and evaluate the content in relation to the specified criteria. Obtain and review documentation demonstrating that management verified the required experience/qualifications of the staff (per management policy). If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.308	§164.308(a)(3): **Workforce Security** - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Establish a Workforce Clearance Procedures	Inquire of management as to whether procedures exist for granting access to ePHI. Obtain and review policy and procedures and evaluate the content in relation to the relevant specified performance criteria. Obtain and review evidence of approval or verification of access to ePHI. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.308	§164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).	Establish Termination Procedures	Inquire of management as to whether there are separate procedures for terminating access to ePHI when the employment of a workforce member ends, i.e., voluntary termination (retirement, promotion, transfer, change of employment) vs. involuntary termination (termination for cause, reduction in force, involuntary transfer). Inquire of management as to whether a standard set of procedures are in place to recover access control devices and deactivate computer access upon termination of employment. Obtain and review policy and procedures for terminating access to ePHI and evaluate the content in relation to the specified performance criteria. Obtain and review evidence of monitoring to determine whether access to	Addressable

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
			ePHI is terminated in a timely manner. Obtain and review a standard set of procedures and evaluate the content in relation to the specified performance criteria. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	
§164.308	§164.308(a)(4): **Information Access Management §164.308(a)(4)(ii)(b)** - Implement policies and procedures for granting access to electronic protected health information; for example, through access to a workstation, transaction, program, process, or other mechanism.	Implement Policies and Procedures for Authorizing Access	Inquire of management as to whether policies and procedures are in place to grant access to ePHI. Obtain and review policies and procedures and evaluate the content relative to the specified criteria for granting access. Determine if the policies and procedures have been approved and updated on a periodic basis. Determine if the entity's IT system has the capacity to set access controls. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so. Evaluate this documentation if applicable.	Addressable
§164.308	§164.308(a)(4): **Information Access Management §164.308(a)(4)(ii)(c)** - Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Implement Policies and Procedures for Access Establishment and Modification	Inquire of management as to whether policies and standards exist to authorize access and document, review, and modify a user's right of access to a workstation, transaction, program, or process. Obtain and review formal documentation and evaluate the content relative to the specified criteria for authorizing access, and for documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process. Determine if policies or standards have been approved and updated on a periodic basis. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so. Evaluate this documentation if applicable.	Addressable
§164.308	§164.308(a)(4)(ii)(A): **Information Access Management** - If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Isolate Healthcare Clearinghouse Functions	Inquire of management as to whether policy and procedures for access are consistent with the HIPAA Security Rule. In the event a clearinghouse exists within the organization, obtain and inspect policies and procedures to understand whether access controls are consistent with the HIPAA Security Rule that protects ePHI from unauthorized access. Determine if policies or practices have been approved and updated on a periodic basis.	Required
§164.308	§164.308(a)(4) **Information Access Management** -	Evaluate Existing Security	Inquire of management as to whether formal or informal policies and procedures exist relating to	Addressable

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Measures Related to Access Controls	the security measures for access controls. Obtain and review formal or informal policies and procedures and evaluate the content in relation to the specified criteria on security measures for access controls. Determine if the formal or informal policies and procedures have been approved and updated on a periodic basis. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on their rational as to why and where they have chosen not to fully implement this specification. Evaluate this documentation if applicable.ci...	
§164.308	§164.308(a)(5) **Security Awareness and Training** - Implement a security awareness and training program for all members of its workforce (including management).	Develop and Approve a Training Strategy and a Plan	Inquire of management as to whether security awareness and training programs address the specific required HIPAA policies. Obtain and review a list of security awareness and training programs and evaluate the content in relation to the specified criteria. Determine if the specific HIPAA policies are addressed in these courses. Determine if the security awareness and training programs are provided to the entire organization. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.308	§164.308(a)(5) **Security Awareness and Training** - Implement a security awareness and training program for all members of its workforce (including management).	Develop and Approve a Training Strategy and a Plan	Inquire of management as to whether security awareness and training programs outline the scope of the program. Obtain and review a sample of security awareness and training programs and evaluate the content in relation to the specified criteria. Determine if security awareness and training programs have been reviewed and approved. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on their rational as to why and where they have chosen not to fully implement this specification. Evaluate this documentation if applicable.	Addressable
§164.308	§164.308(a)(5)(ii)(B): **Security Awareness and Training** - Procedures for guarding against, detecting, and reporting malicious software. §164.308(a)(5)(ii)(c): **Security Awareness and Training** - Procedures for monitoring log-in attempts and reporting discrepancies. §164.308(a)(5)(ii)(d): **Security Awareness and Training** - Procedures for creating, changing, and	Protection from Malicious Software; Log-in Monitoring; and Password Management	Inquire of management as to whether formal or informal policy and procedures exist to inform employees of the importance of protecting against malicious software and exploitation of vulnerabilities. Obtain and review formal or informal policy and procedures for informing employees of the importance of protecting against malicious software and exploitation of vulnerabilities. Determine if the formal or informal policy and procedures have been approved and updated as needed. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this	Addressable

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	safeguarding passwords.		specification and their rationale for doing so....	
§164.308	§164.308(a)(5) **Security Awareness and Training** - Implement a security awareness and training program for all members of its workforce (including management).	Develop Appropriate Awareness and Training Content, Materials, and Methods	Inquire of management as to whether training materials incorporate relevant current IT security topics. Obtain and review a sample of training materials and determine if training materials are updated with relevant and current information. Determine if training materials are reviewed to ensure relevant and current information is included. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.308	§164.308(a)(5) **Security Awareness and Training** - Implement a security awareness and training program for all members of its workforce (including management).	Implement the Training	Inquire of management as to whether employees receive all required training. Obtain and review a list of required training. Determine if required training courses are designed to help employees fulfill their security responsibilities. Determine if training courses are provided to employees to fulfill their security responsibilities. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.308	§164.308(a)(5)(ii)(A): **Security Awareness and Training** - Periodic security updates.	Implement Security Reminders	Inquire of management as to whether security policies and procedures are updated periodically. Obtain and review security policies and procedures. Determine if security policies and procedures are approved and updated on a periodic basis. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.308	§164.308(a)(5) **Security Awareness and Training** - Implement a security awareness and training program for all members of its workforce (including management).	Monitor and Evaluate Training Plan	Inquire of management as to whether training is conducted whenever there are changes in the technology and practices. Obtain and review security awareness and training programs and evaluate the content in relation to the specified criteria. Determine if training materials are updated with new technology and practices. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.308	§164.308(a)(6): **Security Incident Procedures (§164.308(a)(6)(ii))** - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of	Develop and Implement Procedures to Respond to and Report Security Incidents	Inquire of management as to whether there are formal or informal policies and/or procedures in place for identifying, responding to, reporting, and mitigating security incidents. Obtain and review the formal or informal policies and procedures and determine if incident response procedures are in place. Obtain and review the formal or informal policies and/or procedures and	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	security incidents that are known to the covered entity; and document security incidents and their outcomes.		determine if incident response procedures are updated on a periodic basis based on changing organizational needs. Obtain and review formal or informal documentation to determine if the incident response procedures have been communicated to appropriate entity personnel. Obtain and review formal or informal documentation of procedures and evaluate the content relevant to the specified criteria in place for conducting post-incident analysis. Obtain and review formal or informal documentation to determine if post-incident analyses have been conducted.	
§164.308	§164.308(a)(6): **Security Incident Procedures (§164.308(a)(6)(ii))** - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Develop and Implement Procedures to Respond to and Report Security Incidents	Inquire of management as to whether policy or procedures exist regarding identifying, documenting, and retaining a record of security incidents. Obtain and review formal documentation and determine if policies and procedures are in place such that security incidents are identified and documented, and that evidence is retained. Obtain and review formal documentation and determine if security incidents have been identified and documented and management retained detailed evidence of the incidents. Obtain and review formal documentation and determine that the results of post-incident analysis are used to update and revise security policies or controls.	Required
§164.308	§164.308(a)(7): **Contingency Plan §164.308(a)(7)(i)** - A contingency plan must be in effect for responding to system emergencies.	Develop Contingency Planning Policy	Inquire of management as to whether a formal contingency plan with defined objectives exists. Inquire of management as to the process in place for identifying critical applications, data, operations, and manual and automated processes involving ePHI. Obtain and review the contingency plan and evaluate the content relevant to the specified criteria. Determine if the contingency plan defines the overall objectives, framework, roles, and responsibilities of the organization. Determine if the contingency plan has been approved and updated on a periodic basis. Obtain and review the process used to identify critical applications, data, operations, and manual and automated processes involving ePHI to determine if it incorporates the recommended performance criteria. Determine if the process has been approved and updated on a periodic basis.	Required
§164.308	§164.308(a)(7)(ii)(A) - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. Contingency Plan §164.308(a)(7)(ii)(b) -	Data Backup Plan and Disaster Recovery Plan	Inquire of management as to whether disaster recovery and data backup plans exist to restore any lost data. Obtain and review disaster recovery and data backup plans and evaluate the content in relation to the specified criteria. Determine if disaster recovery and data backup plans have been approved and updated on a	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	Establish (and implement as needed) procedures to restore any loss of data.		periodic basis.	
§164.308	§164.308(a)(7)(ii)(C): **Contingency Plan** - Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	Develop and Implement an Emergency Mode Operation Plan	Inquire of management as to whether policy and procedures exist to enable the continuation of critical business processes that protect the security of ePHI while operating in emergency mode. Obtain and review policy and procedures used to enable continuation of critical business processes for the protection of the security of ePHI while operating in emergency mode and evaluate the content in relation to the relevant specified performance criteria. Determine if the policy and procedures have been approved and updated on a periodic basis.	Required
§164.308	§164.308(a)(7)(ii)(D): **Contingency Plan** - Implement procedures for periodic testing and revision of contingency plans.	Testing and Revision Procedure	Inquire of management as to whether policy and procedures exist for periodic testing and revision of contingency plans. Obtain and review policy and procedures used for periodic testing and revision of contingency plans and evaluate the content in relation to the specified criteria. Determine if the policy and procedures have been approved and updated on a periodic basis. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.308	§164.308(a)(7): **Contingency Plan §164.308(a)(7)(i)** - Preventive Measures must be identified.	Identify Preventive Measures	Inquire of management as to how preventive measures are identified and deemed practical and feasible in the organization's given environment. Obtain and review a list of preventive measures and evaluate the content relative to the specified criteria.	Required
§164.308	§164.308(a)(7): **Contingency Plan §164.308(a)(7)(ii)(b)** - Establish (and implement as needed) procedures to restore any loss of data.	Develop Recovery Strategy	Inquire of management as to whether procedures exist for recovering documents from emergency or disastrous events. Obtain and review procedures and evaluate the content in relation to specified criteria for the recovery of documents from emergency or disastrous events. Determine if procedures are approved and updated on a periodic basis.	Required
§164.308	§164.308(a)(7): **Contingency Plan §164.308(a)(7)(ii)(a)** - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. Contingency Plan §164.308(a)(7)(ii)(b) - Establish (and implement as needed) procedures to	Data Backup Plan and Disaster Recovery Plan	Inquire of management as to whether written procedures exist to create and maintain exact copies of ePHI. Obtain and review procedures and evaluate the content in relation to the specified criteria used to create and maintain exact copies of ePHI. Determine if the procedure has been approved and updated on a periodic basis.	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	restore any loss of data.			
§164.308	§164.308(a)(8): **Evaluation** - Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	Determine Whether Internal or External Evaluation Is Most Appropriate	Inquire of management whether evaluations are conducted by internal staff or external consultants. Obtain and review a sample of evaluations conducted within the audit period to determine whether they were conducted by internal staff or external consultants. For evaluations conducted by external consultants, determine if an agreement or contract exists and if it includes verification of consultants' credentials and experience. For evaluations conducted by internal staff, determine if the documentation covers elements from the specified performance criteria.	Required
§164.308	§164.308(a)(8): **Evaluation** - Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule	Inquire of management as to whether policy and procedures exist to ensure an evaluation considers all elements of the HIPAA Security Rule. Obtain and review policy and procedures used and evaluate the content in relation to the specified criteria. Determine if the process has been approved and updated on a periodic basis as required.	Required
§164.308	§164.308(a)(8): **Evaluation** - Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	Conduct Evaluation	Inquire of management as to whether policy and procedures exist to ensure all necessary information needed to conduct an evaluation is obtained and documented in advance. Obtain and review the evaluation process in place in relation to the specified criteria. Determine if the policy and procedures have been approved and updated on a periodic basis.	Required
§164.308	§164.308(a)(8): **Evaluation** - required covered entities to periodically conduct an evaluation of their security safeguards to	Document Results	Inquire of management as to whether formal or informal policy and procedures exist to document the evaluation of findings, remediation options and recommendations, and remediation decisions. Obtain and review formal or informal	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their information.		policy and procedures used to document the evaluation of findings, remediation options and recommendations, and remediation decisions in relation to the specified criteria. Determine if written reports of findings are reviewed and approved.	
§164.308	§164.308(a)(8): **Evaluation** - required covered entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their information.	Repeat Evaluations Periodically	Inquire of management as to whether formal or informal security policies and procedures specify that evaluations will be repeated when environmental and operational changes are made that affect the security of ePHI. Obtain and review the entity's formal or informal security policies and procedures and evaluate the content in relation to the specified criteria to determine the process for repeat evaluations. Determine if formal or informal security policies and procedures are reviewed on a periodic basis.	Required
§164.308	§164.308(b)(1): **Business Associate Contracts and Other Arrangements** - Covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in $160.103. The covered entity must obtain satisfactory assurance from the business associate that it will appropriately safeguard the information in accordance with §164.314(a)(1) standards.	Written Contract or Other Arrangement	Inquire of management as to whether a process exists to ensure contracts or agreements include security requirements to address confidentiality, integrity, and availability of ePHI. Obtain and review the documentation of the process used to ensure contracts or arrangements include security requirements to address confidentiality, integrity, and availability of ePHI and evaluate the content in relation to the specified criteria. Determine if the contracts or arrangements are reviewed to ensure applicable requirements are addressed.	Required
§164.308	§164.314: **Business Associate Contracts and Other Arrangements** - If a covered entity enters into other arrangements with another governmental entity that is a business associate, such	Implement An Arrangement Other than a Business Associate Contract if Reasonable and	Inquire of management as to whether a process exists to identify federal, state, or local government business associates. Obtain and review the process used to identify federal, state or local government business associates and evaluate the content in relation to the specified criteria.	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	arrangements may omit provisions equivalent to the termination authorization required by the business associate contract, if inconsistent with the statutory obligation of the covered entity or its business associate. If other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of the standards in this section, a contract or agreement is not required.	Appropriate		
§164.310	§164.310(a)(2)(ii): **Facility access controls** - Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Conduct an Analysis of Existing Physical Security Vulnerabilities	Inquire of management as to whether formal or informal policies and procedures exist regarding access to and use of facilities and equipment that house ePHI. Obtain and review formal or informal policies and procedures and evaluate the content in relation to the relevant specified performance criteria regarding access to and use of facilities and equipment that house ePHI. Determine if formal or informal polices and procedures have been approved and updated on a periodic basis. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.310	§164.310(a)(2)(ii): **Facility access controls** - Implement policies and procedures to safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft.	Develop a Facility Security Plan	Inquire of management as to whether formal or informal policies and procedures exist to safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft. Obtain and review formal or informal policies and procedures and evaluate the content in relation to the specified criteria for safeguarding the facility and equipment therein from unauthorized physical access, tampering, and theft. Determine if policies and procedures have been approved and updated on a periodic basis. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.310	§164.310(a)(2)(i): **Facility access controls** - Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data	Establish Contingency Operations Procedures	Inquire of management as to whether procedures exist for controlling access by staff, contractors, visitors, and probationary employees. Obtain and review formal or informal policies and procedures and evaluate the content in relation to the specified criteria for controlling access by staff,	Addressable

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	under the disaster recovery plan and emergency mode operations plan in the event of an emergency.		contractors, visitors, and probationary employees. Determine if policy and procedures have been approved and updated on a periodic basis. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	
§164.310	§164.310(a)(2)(i): **Facility access controls** - Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Establish Contingency Operations Procedures	Inquire of management to determine if formal or informal documentation exists that allow facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency. Obtain and review formal or informal documentation and evaluate the content in relation to the specified criteria that allow facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan. Determine if formal or informal policy(ies) or practices have been approved and updated on a periodic basis. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.310	§164.310(a)(2)(iV): **Facility access controls** - Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Maintain Maintenance Records	Inquire of management as to whether policies and procedures exist to document repairs and modifications to the physical components of a facility that are related to security. Obtain and review policy and procedures and evaluate the content in relation to the specified criteria for documenting repairs and modifications to the physical components of a facility related to security. Determine if policies and procedures have been approved and updated on a periodic basis. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.310	§164.310(b): **Workstation Use** - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Identify Workstation Types and Functions or Uses	Inquire of management as to whether a process exists for identifying workstations by type and location. Obtain and review formal or informal policies and procedures and evaluate the content in relation to the specified criteria for identifying workstations by type and location. Determine if each workstations is classified based on the capabilities, connection, and allowable activities.	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
§164.310	§164.310(b): **Workstation Use** - Covered entities must identify expected Performance of Each type of workstation.	Identify Expected Performance of Each Type of Workstation	Inquire of management as to whether formal or informal policies and procedures exist related to the proper use and performance of workstations. Obtain and review formal or informal policies and procedures and evaluate the content in relation to the specified criteria for the proper use and performance of workstations. Determine if polices and procedures are approved and updated on a periodic basis.	Required
§164.310	§164.310(b): **Workstation Use** - Covered entities should analyze physical surroundings for physical attributes.	Analyze Physical Surroundings for Physical Attributes	Inquire of management if formal or informal policies and procedures exist to prevent or preclude unauthorized access to an unattended workstation, limit the ability of unauthorized persons to view sensitive information, and dispose of sensitive information as needed. Obtain and review formal or informal policies and procedures and evaluate the content in relation to the specified criteria for monitoring unauthorized access of unattended workstations and limit access to view sensitive information. Determine if formal or informal policies and procedures are approved and updated on a periodic basis.	Required
§164.310	§164.310(c): **Workstation Security §164.310(b)** - Covered entities should implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.	Identify All Methods of Physical Access to Workstations	Inquire of management as to how workstations are physically restricted to limit access to only authorized personnel. Obtain and review formal or informal policies and procedures on how physical access is restricted to appropriate personnel to determine if the policies and procedures include the required security measures and guidance on how to maintain physical security. Obtain and review an inventory of the types and locations of workstations to determine if an inventory exists, when it was last updated, and whether there is a documented process for updating the information. Observe the workstations and the location of workstations to determine if they are located in secure areas and protected with physical security controls such as, cable locks and privacy screens. Observe the premises to determine if doors have locks, cameras are in place, security guards are in place, etc.	Required
§164.310	§164.310(c): **Workstation Security §164.310(b)** - Covered entities should implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Identify and Implement Physical Safeguards for Workstations	Inquire of management as to what physical security measures are in place to prevent unauthorized access to restricted information. Observe the workstations and the locations of workstations to determine if they are located in secure areas, if laptops are used, if system timeouts are used, and if workstations are protected by password or some alternative authentication. Obtain and review a list of employees. For a selection of employees, determine how the physical security policy is communicated and how the user acknowledges	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
			the information contained within. Observe the premises to determine if doors have locks, cameras are in place, security guards are in place, etc.	
§164.310	§164.310(d)(1): **Device and Media Controls** - §164.310(d)(2)(i) Implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored.	Implement Methods for Final Disposal of ePHI	Inquire of management as to how the disposal of hardware, software, and ePHI data is managed. Obtain and review formal policies and procedures and evaluate the content relative to the specified criteria regarding the disposal of hardware, software, and ePHI data. Obtain evidence, on a sample basis, to determine whether the entity had oversight policies and procedures that address how management verifies that disposal policies are being carried out.	Required
§164.310	§164.310(d)(1): **Device and Media Controls** - §164.310(d)(2)(iii) Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Maintain Accountability for Hardware and Electronic Media	Inquire of management as to how the location and movement of media and hardware containing ePHI is tracked. Obtain and review policies and procedures and evaluate the content relative to the specified criteria regarding tracking the location of ePHI media and hardware. Obtain and review documentation and evaluate the content relative to the specified criteria to determine media and hardware that contain ePHI are tracked. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on their rational as to why and where they have chosen not to fully implement this specification. Evaluated this documentation if applicable.	Addressable
§164.310	§164.310(d)(1): **Device and Media Controls** - §164.310(d)(2)(iv) Create a retrievable exact copy of ePHI, when needed, before movement of equipment.	Develop Data Backup and Storage Procedures	Inquire of management as to the procedures established over the backup and restoration of ePHI data. Obtain and review formal or informal policies and procedures and evaluate the content relative to the specified criteria to determine whether procedures cover the backup and restoration of ePHI data. Obtain and review formal or informal documentation and evaluate the content to identify where ePHI data are stored. If data is stored onsite, observe the facility to determine if the location is secure and protected from the elements, e.g., the location is equipped with a fire suppression system, a fireproof safe, etc. If data is stored off-site, obtain and review documentation and evaluate the content relative to the criteria specified to determine if the data is stored in a secure location, e.g., a contract with a service provider such as Iron Mountain, a SSAE16 report over the controls in place if the service is a third-party provider, etc. If the off-site location is run by the entity, observations similar to the ones listed above may need to be performed. For a selection of days, obtain and review evidence that backups over ePHI data were performed successfully. Obtain and review formal or informal policies and	Addressable

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
			procedures and evaluate the content relative to the specified criteria to determine how often restoration tests are to be completed. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so. Evaluate this documentation if applicable.	
§164.310	§164.310(d)(1): **Device and Media Controls** - §164.310(d)(2)(iv) Create a retrievable exact copy of ePHI, when needed, before movement of equipment.	Develop Data Backup and Storage Procedures	Inquire of management as to the procedures established over the backup and restoration of ePHI data. Obtain and review formal or informal policies or procedures and evaluate the content in relation to the specified criteria to determine whether procedures cover the backup and restoration of ePHI data. Obtain and review documentation and evaluate the content to understand where ePHI data are stored. If data is stored onsite, observe the facility to determine if the location is secure and protected from the elements, e.g., the location is equipped with fire suppression system, fireproof safe, etc. If data is stored off-site, obtain and review documentation and evaluate the content in relation to the specified criteria to determine if the data is stored in a secure location, e.g., a contract with a service provider such as Iron Mountain, a SSSAE 16 report over the controls in place if the service is a third-party provider. If the off-site location is run by the entity, observations similar to the ones above may need to be made. For a selection of days, obtain and review evidence that backups over ePHI data were performed successfully. Obtain and review policies or procedures and evaluate the content in relation to the specified criteria to determine how often restoration tests are completed. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.	Addressable
§164.310	§164.310(d)(1): **Device and Media Controls** - §164.310(d)(2)(ii) Implement procedures for removal of ePHI from electronic media before the media are made available for reuse. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record	Develop and Implement Procedures for Reuse of Electronic Media	Inquire of management as to the processes established to remove ePHI before reusing electronic media and who is responsible for the overseeing those processes. Obtain and review policies and procedures and evaluate the content in relation to the specified criteria for removing ePHI from electronic media before they are issued for reuse.	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	new information.			
§164.312	§164.312(a)(1): **Access Control** - §164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.	Encryption and Decryption	Inquire of management as to whether an encryption mechanism is in place to protect ePHI. Obtain and review formal or informal policies and procedures and evaluate the content relative to the specified criteria to determine that encryption standards exist to protect ePHI. Based on the complexity of the entity, elements to consider include but are not limited to: -Type(s) of encryption used. -How encryption keys are protected. -Access to modify or create keys is restricted to appropriate personnel. -How keys are managed. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so. Evaluate this documentation if applicable.	Addressable
§164.312	§164.312(a)(1): **Access Control** - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Analyze Workloads and Operations to Identify the Access Needs of All Users	Inquire of management as to how the workloads and operations are analyzed to determine the access needs of all users within the entity. Obtain and review documentation of the analysis performed to determine the access needs of the entity's users and evaluate the content in relation to the specified criteria.	N/A
§164.312	§164.312(a)(1): **Access Control** - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Identify Technical Access Control Capabilities	Inquire of management as to how technical access control capabilities are defined. Obtain and review evidence to determine whether and how technical access capabilities are defined for in-scope systems. Obtain and review screenshots from in-scope systems to determine whether technical access capabilities are defined, i.e., read-only, modify, full-access.	N/A
§164.312	§164.312(a)(2)(i): **Access Control** - Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.	Ensure that All System Users Have Been Assigned a Unique Identifier	Inquire of management as to how users are assigned unique user IDs. Obtain and review policies and/or procedures and evaluate the content in relation to the specified criteria to determine how user IDs are to be established and assigned and evaluate the content in relation to the specified criteria. Obtain and review user access lists for each in-scope application to determine if users are assigned a unique ID and evaluate the content in relation to the specified criteria for attributing IDs. For selected days, obtain and review user access logs to determine	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
			if user activity is tracked and reviewed on a periodic basis and evaluate the content of the logs in relation to the specified criteria for access reviews.	
§164.312	§164.312(a)(1): **Access Control** - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Develop Access Control Policy	Inquire of management to determine if there is an access control policy in place. Obtain and review policies and/or procedures and evaluate the content in relation to the specified criteria to determine if a formal policy is in place over access control and evaluate the content in relation to the specified criteria.	N/A
§164.312	§164.312(a)(1): **Access Control** - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Implement Access Control Procedures Using Selected Hardware and Software	Inquire of management as to what access control procedures are in place. Obtain a list of new hires within the audit period. For a selection of new hires, obtain and review user access authorization forms for evidence of approval and evaluate the content of the forms in relation to the specified criteria.	N/A
§164.312	§164.312(a)(1): **Access Control** - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Implement Access Control Procedures Using Selected Hardware and Software	Inquire of management as to how generic and system IDs are implemented. Obtain and review policies and/or procedures and evaluate the content in relation to the specified criteria to determine the formal procedures in place over creating generic and system IDs. Obtain and review user access listings to determine how many generic and/or system IDs are in use. For a selection of generic and/or system IDs in use or created within the audit period, obtain and review the approval forms for each and evaluate the content in relation to the specified criteria for approvals.	N/A
§164.312	§164.312(a)(1): **Access Control** - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Implement Access Control Procedures Using Selected Hardware and Software	Inquire of management as to who has access to add, modify, or delete user access. Obtain and review policies and/or procedures and evaluate the content in relation to the specified criteria to determine who has the ability to add, modify, or delete user access. Obtain and review a list of users with privileged access to determine their access is appropriate based on policy in place.	N/A

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
§164.312	§164.312(a)(1): **Access Control** - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Review and Update User Access	Inquire of management as to whether user access to systems and applications is reviewed on a periodic basis. Obtain and review policies and/or procedures to determine whether formal procedures are in place over the review of user access that address the recommended performance criteria, such as enforcing the policies and procedures as a matter of ongoing operations; determining whether changes are needed based on periodic reviews; and establishing and updating access. Obtain and review documentation to determine whether reviews have been performed over user access and evaluate the content in relation to the specified criteria for reviews.	N/A
§164.312	§164.312(a)(2)(ii): **Access Control** - Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. Identify a method of supporting continuity of operations should the normal access procedures be disabled or unavailable due to system problems.	Establish an Emergency Access Procedure	Inquire of management as to whether an emergency access procedure is in place for obtaining necessary ePHI during an emergency. Obtain and review policies and/or procedures and evaluate the content in relation to the specified criteria to determine if an emergency access procedure is in place for obtaining necessary ePHI during an emergency.	Required
§164.312	§164.312(a)(2)(ii): **Access Control -** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. Identify a method of supporting continuity of operations should the normal access procedures be disabled or unavailable due to system problems.	Establish an Emergency Access Procedure	Inquire of management as to whether and how access to initiate the emergency access process is limited to appropriate personnel. Obtain and review a list of individuals with access to initiate the emergency access procedures and obtain evidence indicating whether a selection of the individuals has the qualifications and training over ePHI, per management's policy or process.	Required
§164.312	§164.312(a)(2)(iii): **Access Control** - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Automatic Logoff	Inquire of management as to whether automatic logoff occurs after a predetermined time of inactivity. Obtain and review policies and/or procedures and evaluate the content in relation to the specified criteria to determine whether they specify that automatic logoff occurs after a predetermined time of inactivity. Obtain and review screenshots to determine that automatic logoff settings are implemented and conform to the established policies and/or procedures. Obtain and review screenshots of the encryption configuration over ePHI.	Addressable
§164.312	§164.312(a)(1):	Terminate	Inquire of management as to how user access is	N/A

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	Access Control - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Access if it is No Longer Required	removed upon termination or change of position on a timely basis. Obtain and review policies and/or procedures and evaluate the content in relation to the specified criteria to determine how user access is terminated. Obtain and review a list of terminations and job transfers within the audit period from Human Resources. Obtain and review a list of active users within each system and application to determine the terminated users'/transfers' access was removed from each application to which they had access. (For ""job transfers"" some access may remain. The appropriateness of user access is tested elsewhere and does not need to be tested here as part of this step for ""job transfers."") Obtain and review the user termination forms to determine their access was removed on a timely basis.	
§164.312	§164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Determine the Activities that Will be Tracked or Audited	Inquire of management as to whether audit controls have been implemented over information systems that contain or use ePHI. Obtain and review documentation relative to the specified criteria to determine whether audit controls have been implemented over information systems that contain or use ePHI.	Required
§164.312	§164.312(b) **Audit Controls** - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Select the Tools that Will be Deployed for Auditing and System Activity Reviews	Inquire of management as to whether systems and applications have been evaluated to determine whether upgrades are necessary to implement audit capabilities. Obtain and review documentation of tools or applications that management has identified to capture the appropriate audit information.	Required
§164.312	§164.312(b) **Audit Controls** - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Develop and Deploy the Information System Activity Review/Audit Policy	Inquire of management as to whether a formal or informal audit policy is in place to communicate the details of the entity's audits and reviews to the work force. Obtain and review formal or informal policies and procedures and evaluate the content in relation to the specified criteria to understand whether a formal audit policy is in place to communicate the details of the entity's audits and reviews to the work force. Obtain and review an email, or some form of communication, showing that the audit policy is communicated to the work force. Alternatively, a screenshot of the audit policy located on the entity's intranet would suffice.	Required
§164.312	§164.312(b) **Audit Controls** - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use	Develop Appropriate Standard Operating Procedures	Inquire of management as to whether procedures are in place on the systems and applications to be audited and how they will be audited. Obtain and review management's procedures in place to determine the systems and applications to be audited and how they will be audited.	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	electronic protected health information.			
§164.312	§164.312(c)(1) Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Identify All Users Who Have Been Authorized to Access ePHI	Inquire of management as to whether all users who should have access to ePHI have been identified. Obtain and review the documentation management uses to determine whether users who should have access to ePHI have been identified and evaluate this documentation against specified criteria.	N/A
§164.312	§164.312(c)(1) **Integrity** - Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Implement Procedures to Address These Requirements	Inquire of management as to whether access control procedures are in place. Obtain and review policies and procedures and evaluate the content in relation to the specified criteria to determine whether formal procedures over access control exist. Obtain and review a list of new hires within the audit period. For a selection of new hires, obtain and review user access authorization forms to determine that access is approved per management's requirements.	N/A
§164.312	§164.312(c)(2) - Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Implement a Mechanism to Authenticate ePHI	Inquire of management as to whether electronic mechanisms are in place to authenticate ePHI. Obtain and review documentation and evaluate the content relative to the specified criteria to determine that electronic mechanisms are in place to authenticate ePHI. Obtain and review screenshots of the technology in place to determine whether a solution has been implemented and is in effect. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so. Evaluate this documentation if applicable.	Addressable
§164.312	Identify methods available for authentication. Under the HIPAA Security Rule, authentication is the corroboration that a person is the one claimed (45 CFR § 164.304). Authentication requires establishing the validity of a transmission source and/or verifying an individual's claim that he or she has been authorized for specific access privileges to information and information systems.	Determine Authentication Applicability to Current Systems /Applications	Inquire of management as to the authentication methods that have been identified for the entity's systems and applications. Obtain and review documentation to determine whether the applications requiring authentication have been identified and whether authentication methods have been researched and identified for the entity's systems and applications that require authentication.	Required
§164.312	§164.312(d): **Person or Entity Authentication** - Weigh the relative advantages and disadvantages of commonly used authentication	Evaluate Authentication Methods Available	Inquire of management as to how authentication methods have been evaluated for the entity's systems and applications to assess strengths and weaknesses and the cost to benefit ratio of different types of authentication in order to establish an appropriate level of authentication.	Required

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification
	approaches. There are four commonly used authentication approaches available: -Something a person knows, such as a password. -Something a person has or is in possession of, such as a token (smart card, ATM card, etc.). -Some type of biometric identification a person provides, such as a fingerprint. -A combination of two or more of the above approaches.		Obtain and review documentation related to the determination of strengths and weaknesses and cost to benefit ratio to determine whether the authentication methods have been evaluated for the entity's systems and applications and evaluate the content in relation to the specified criteria.	
§164.312	§164.312(d): **Person or Entity Authentication** - Consider the results of the analysis conducted under Key Activity 2, above, and select appropriate authentication methods. Implement the methods selected into your operations and activities.	Select and Implement Authentication Option	Inquire of management as to whether a formal authentication policy is in place for the entity's systems and applications. Obtain and review documentation and evaluate the content in relation to the specified criteria to determine whether a formal authentication policy is in place for the entity's systems and applications that includes the minimum requirements for the chosen authentication types and how to use each authentication method. Obtain and review screenshots of the availability of the authentication policy to the work force to determine if the policy is readily available.	Required
§164.312	§164.312(d): **Person or Entity Authentication** - Consider the results of the analysis conducted under Key Activity 2, above, and select appropriate authentication methods. Implement the methods selected into your operations and activities.	Select and Implement Authentication Option	Inquire of management as to how the authentication system is periodically tested and upgraded when upgrades are available. Obtain and review documentation and evaluate the content in relation to the specified criteria to determine the authentication system is periodically tested and upgraded when upgrades are available. Obtain and review a log of testing results and upgrades to determine if testing is performed and upgrades are applied.	Required
§164.312	§164.312(e)(1) **Transmission Security** - Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Develop and Implement Transmission Security Policy and Procedures	Inquire of management as to the formal ePHI data transmission policy in place for the entity. Obtain and review the formal ePHI data transmission policy in place for the entity and evaluate the content in relation to the specified criteria.	N/A

HIPAA Privacy Rule

Section	Established Performance Criteria	Key Activity	Audit Procedures
§164.502	§164.502 - Uses and disclosures of protected health information: general rules A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.	Deceased individuals	Inquire of management as to whether requirements with respect to PHI of a deceased person are met. Obtain and review the process and evaluate the content relative to the specified criteria used to ensure compliance with the requirements of PHI with respect to a deceased person.
§164.502	§164.502 - Uses and disclosures of protected health information: general rules §164.502(g)(2) - If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation. §164.502(g)(3)(i) - If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if: (a) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative; (b) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or (c) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service. §164.502(g)(3)(ii) - Notwithstanding the provisions of paragraph (g)(3)(i) of this section: (a) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with §164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; (b) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with	Personal representatives	Inquire of management as to whether requirements with respect to personal representatives are met. Obtain and review the process and evaluate the content relative to the specified criteria used to ensure compliance with the requirements of PHI with respect to personal representatives.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	§164.524 to , protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and (c) Where the parent, guardian, or other person acting in loco parentis, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (c) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under §164.524 to a parent, guardian, or other person acting in loco parentis, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.		
§164.502	§164.502 A covered entity that is required by §164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by §164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in §164.520(b)(1)(iii)(a)-(c), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.	Uses and disclosures consistent with notice	Inquire of management as to whether uses and disclosures are consistent with notice. Obtain and review the process and evaluate the content in relation to the specified criteria to determine if the process for uses and disclosures is consistent with notice.
§164.502	§164.502 A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that: (i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and (ii) The disclosure is to: (a) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or (b) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.	Disclosures by whistleblowers	Inquire of management as to whether a process exists to permit disclosures of PHI by whistleblowers and the conditions under which whistleblowers may disclose PHI. Obtain and review the process and evaluate the content in relation to the specified criteria to determine how the entity evaluates whether disclosures of PHI are due to whistleblowers.
§164.502	§164.502(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that: (i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and (ii) The protected health information disclosed is limited to the information listed in §164.512(f)(2)(i).	Disclosures by workforce members who are victims of a crime	Inquire of management as to whether a process exists to permit certain disclosures of PHI by workforce members who are victims of a crime and the conditions under which they may disclose PHI. Obtain and review the process and evaluate the

Section	Established Performance Criteria	Key Activity	Audit Procedures
			content in relation to the specified criteria to determine how the entity ensures disclosures of PHI are due to victims of a crime. NOTE: Entities are not required to have processes in place for these disclosures, although it might be helpful for an entity to create one for workforce members who are crime victims.
§164.502	§164.502 - Uses and disclosures of protected health information: general rules §164.502(h) - A covered health care provider or health plan must comply with the applicable requirements of §164.522(b) in communicating protected health information. §164.522(b)(1)(i) - A covered entity must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations. §164.522(b)(1)(ii) - A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative location, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.	Confidential communications	Inquire of management as to whether a process exists to ensure the entity complies with confidential communications requirements. Obtain and review the process and evaluate the content to determine if the entity complies with confidential communication requirements.
§164.504	§164.504 - Uses and disclosures: Organizational requirements The contract or other arrangement between the covered entity and the business associate required by §164.502 must meet the requirements of the following, as applicable. -A contract between the covered entity and a business associate must: (i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity except that: (A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate; and (B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity. (ii) Provide that the business associate will: (A) Not use or further disclose the information other than as permitted or required by the contract or as required by law; (B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract; (C) Report the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware; (D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of,	Business associate contracts	Inquire of management as to whether a business associate contract permits the use and disclosure of PHI for the proper management and administration of the business associate. Obtain and review formal or informal policies and procedures related to business associate agreements. Obtain and review formal or informal policies and procedures and evaluate the content relative to the specified criteria for identifying whether a business associate agreement is required. Verify whether the agreement limits uses and disclosures to those that are permitted by the standard. Obtain and

Section	Established Performance Criteria	Key Activity	Audit Procedures
	the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information; (E) Make available protected health information in accordance with §164.524; (F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526; (G) Make available the information required to provide an accounting of disclosures in accordance with §164.528; (H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and (iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. If a covered entity and its business associate are both governmental entities: (A) The covered entity may comply with this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of this section. (B) The covered entity may comply with this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of this section. If a business associate is required by law to perform a function or activities on behalf of a covered entity or to provide a service described in the definition of business associate in §160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by this section, if such attempts fails, documents the attempt and the reasons that such assurances cannot be obtained. The covered entity may omit from its other arrangements the termination authorization required by this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.		review a business associate agreement and evaluate the content relative to the specified criteria.
§164.504	§164.504 - Uses and disclosures: Organizational requirements (i) Except as provided under paragraph (ii) or (iii) of this section or as otherwise authorized under §164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart. (ii) The group health plan, or a health insurance issuer or HMP with respect to the group plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of: (A)Obtaining premium bids from health plans for providing health insurance coverage under the	Requirements for group health plans	Inquire of management as to whether the plan documents restrict the use and disclosure of PHI by the plan sponsor. Obtain and review a sample of plan documents. Verify if the use and disclosure of PHI by the plan sponsor is restricted. Verify what information the sponsor does obtain and how it is used.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	group health plan; or (B) Modify, amending, or terminating the group health plan. (iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMP offered by the plan.		
§164.504	§164.504(g) Requirements for a covered entity with multiple covered functions. (1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements (do global search on requirements for ""require"" to make sure spelling is correct) , and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed. (2)A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for the purposes related to the appropriate function being performed.	Requirements for a covered entity with multiple covered functions	Inquire of management as to whether the entity has multiple functions and if the use and disclosure of PHI is only for the purpose related to the appropriate function being performed. Obtain and review formal documentation and evaluate the content in relation to the specified criteria for restricting the use and disclosure of PHI to only the purpose related to the appropriate function being performed. Verify that formal documentation restricts the use and disclosure of PHI to only the purpose related to the appropriate function being performed. Determine if the formal documentation has been approved and updated on a periodic basis.
§164.506	§164.506 - Uses and disclosures to carry out treatment, payment, or health care operations §164.506(a) Except with respect to uses or disclosures that require an authorization under §164.506(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.	Permitted uses and disclosures	Inquire of management as to whether a process exists for the use or disclosure of PHI for treatment, payment, or health care operations provided and whether such use or disclosure is consistent with other applicable requirements. Obtain and review the process and evaluate the content relative to the specified criteria used for use or disclosure of PHI for treatment, payment, ,or health care operations provided to determine whether such use or disclosure is consistent with other applicable

Section	Established Performance Criteria	Key Activity	Audit Procedures
			requirements. Obtain and review a sample of training programs and evaluate the content relative to the specified criteria to determine the use or disclosure of PHI for treatment, payment, or health care operations provided is consistent with other applicable requirements.
§164.506	§164.506 - Uses and disclosures to carry out treatment, payment, or health care operations §164.506(b)(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations. §164.506(b)(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under §164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.	Consent for uses and disclosures	Inquire of management as to whether the entity has determined that obtaining the individual's consent is necessary. Obtain and review policies and procedures and evaluate the content in relation to the specified criteria related to consent for uses and disclosures: -Confirm that a consent is not used in place of a valid authorization for uses and disclosures that would require an authorization.
§164.508	§164.508 - Uses and disclosures for which an authorization is required §164.508(b)(6) A covered entity must document and retain any signed authorization under this section as required by §164.530(j). §164.508(c)(1) A valid authorization must contain core elements. §164.508(c)(2) In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following: (i) The individual's right to revoke the authorization in writing. (ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization. (iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient can no longer be protected by this subpart. §164.508(c)(3) The authorization must be written in plain language. §164.508(c)(4) If a covered entity seeks an authorization form an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization. §164.508(b)(1)(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section, applicable. (ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided, that such additional elements or information are not inconsistent with the elements are not inconsistent with the elements required by this section. §164.508(b)(2) An authorization is not valid, if the document submitted has any of the following defects: (i) The	Obtaining Authorization as Required for Internal Use and Disclosure of Protected Health Information	Inquire of management as to whether a process exists to determine when authorization is required. Obtain and review a sample of instances where authorization is required to determine if a valid authorization was obtained: -Evidence that an authorization was valid. For providers only: obtain and review all patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	expiration data has passed or the expiration event is known by the covered entity to have occurred; (ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable; (iii) The authorization is known by the covered entity to have been revoked; (iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable; (v) Any material information in the authorization is known by the covered entity to be false.		
§164.508	§164.508 - Uses and disclosures for which an authorization is required §164.508(a)(1) Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization. §164.508(a)(2) Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes. §164.508(a)(3) Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing.	Authorizations for uses and disclosures is required	Inquire of management as to whether formal or informal policies and procedures exist for obtaining a valid authorization. Obtain and review polices and procedures and evaluate the content relative to the specified criteria to ensure that a valid authorization is obtained: -Evidence of covered entity policy -Evidence of covered entity valid authorization Determine if the Provider/Plan policy has been approved and updated on a periodic basis.
§164.508	§164.508(b)(3)An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows: (i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research; (ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes; (iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.	Compound authorizations	Inquire of management as to whether the covered entity uses or discloses PHI for the purpose of research, provides research and/or psychotherapy services, or uses compound authorizations. Inquire of management as to whether PHI being disclosed pursuant to an authorization is a psychotherapy note. Obtain and review a list of authorizations and evaluate the content in relation to the specified criteria to determine if the compound authorizations are appropriate.
§164.508	§164.508(b)(4) A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except: (i) A covered health care provider may	Prohibition on conditioning of authorizations	Inquire of management as to when the entity can condition the provision to an individual of treatment,

Section	Established Performance Criteria	Key Activity	Audit Procedures
	condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section; (ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if: (A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and (B) The Authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and (iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.		payment, enrollment in the health plan, or eligibility for benefits. Obtain and review privacy practices and evaluate the content in relation to the specified criteria to determine if treatment, payment, enrollment, or eligibility is conditioned in the documents: -Evidence of provider/payer health plan conditions
§164.510	§164.510 - Uses and disclosures requiring an opportunity for the individual to agree or to object §164.510(b)(3) If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescription, medical supplies, X-rays, or other similar forms of protected health information.	Limited uses and disclosures when the individual is not present	Inquire of management as to whether a process exists for disclosing only information relevant to the person's involvement with the individual's health care. Obtain and review the process used for disclosing only information relevant to the person's involvement with the individual's health care: -Evidence of covered entity process. Obtain evidence that staff have been trained to carry out this standard.
§164.510	§164.510(a)(1) Except when an objection is expressed in accordance with paragraph (a)(2) or (3) of this section, a covered health care provider may: (i) Use the following protected health information to maintain a directory of individuals in its facility: (A) The individual's name; (B) The individual's location in the covered health care provider's facility; (C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and (D) The individual's religious affiliation; and (ii) Disclosure for directory purposes such information: (A) To member of the clergy; or (B) Except for religious affiliation, to other persons who ask for the individual by name.	Use and Disclosure for Facility Directories	Inquire of management as to whether the entity maintains a directory of individuals in its facility. Obtain and review a directory of individuals in the entity's facility and evaluate the content in relation to the relative specified criteria to determine the disclosure and purpose of such information is appropriate. -Evidence of Provider/Payer directory Determine if Provider/Payer directory is updated on a periodic basis.

Section	Established Performance Criteria	Key Activity	Audit Procedures
§164.510	§164.510(a)(3)(i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory.	Uses and Disclosures for Facility Directories in Emergency Circumstances	Inquire of management as to whether a process exists to use or disclose PHI for the facility directory due to an emergency treatment. Obtain and review the process used to disclose PHI for the facility directory due to an emergency treatment: -Evidence of provider/payer process Determine if disclosure of PHI for the facility directory due to an emergency treatment is appropriate.
§164.510	§164.510(b)(1)(i) A covered entity may, in accordance with paragraphs (b)(2) or (b3) of this section, disclose to a family member, or other relative, or a close personal friend of the individual, or any other person identified by the individual, protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. §164.510(b)(1)(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b(2),(3), or (4) of this section, as applicable.	Permitted uses and disclosers	Inquire of management as to what the process is for disclosing PHI to family members, relatives, close personal friends or other persons identified by the individual. Obtain and review applicable policies and procedures for such disclosures.
§164.510	§164.510(b)(2) If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it: (i) Obtains the individual's agreement; (ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or (iii) Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.	Uses and disclosures with the individual present	Inquire of management as to how the entity discloses PHI to persons involved in the individual's care when the individual is present, and whether the entity can disclose PHI with the individual present. Obtain and review a process for disclosure of PHI with the individual present to determine its appropriateness: -Evidence of provider/payer process
§164.510	§164.510(b)(4) A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraph (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the	Uses and disclosures for disaster relief purposes	Inquire of management as to whether a process exists for disclosing PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. Obtain and

Section	Established Performance Criteria	Key Activity	Audit Procedures
	covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.		review policies and procedures and evaluate the content in relation to the relative specified criteria related to mandatory reporting: - Evidence of covered entity Provider/Payer process Determine if the covered entity Provider/Payer process for disclosing PHI for disaster relief purposes is appropriate.
§164.510	§164.510 - Uses and disclosures requiring an opportunity for the individual to agree or to object §164.510(a)(2) A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.	Opportunity to Object	Inquire of management as to whether objections by individuals to restrict or prohibit some or all of the uses or disclosures are obtained and maintained. Obtain and review Notice of Privacy Practices and evaluate the content in relation to the specified criteria for evidence of opportunity to object. Obtain evidence that staff have been trained to properly carry out this standard.
§164.512	§164.512 - Uses and disclosures for which an authorization or opportunity to agree or object is not required §164.512(e) - A covered entity may disclose protected health information in the course of any judicial or administrative proceeding: (i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or (ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if: (a) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party of the protected health information that has been requested has been given notice of the request; or (b) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section. (iii) For the purpose of paragraph (e)(1)(ii)(a) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that: (a) The party requesting such information	Disclosures for judicial and administrative proceedings	Inquire of management as to whether a process exists to determine if the disclosure of PHI in the course or any judicial or administrative proceeding is appropriate. Obtain and review formal or informal policy and procedures related to disclosures of PHI made pursuant to judicial and administrative proceedings Obtain and review a sample of disclosures and the corresponding court orders, subpoenas, or discovery requests for judicial and administrative proceedings and determine if disclosures are appropriate. Based on the complexity of the entity, elements to consider include, but are not limited

Section	Established Performance Criteria	Key Activity	Audit Procedures
	has made a good faith attempts to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address); (b) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and (c) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and (1) No objections were filed; or (2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution. (iv) For the purpose of paragraph (e)(1)(ii)(b) of this section, a covered entity receives satisfactory assurance from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that: (a) The parties to the dispute given rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over and dispute; or (b) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal. (v) For purpose of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court of an administrative tribunal r stipulation by the parties to the litigation or administrative proceeding that: (a) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and (b) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding. (vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(a)(b) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.		to, whether the disclosure of PHI: -Is in response to an order of a court or administrative tribunal. -Is in response to a subpoena, discovery request, or other lawful process. Verify disclosure of PHI in the course of any judicial or administrative proceeding is appropriate. Elements to consider should consist of performance criteria and include, but are not limited to: -A court order requesting a response. -A subpoena.
§164.512	§164.512 - Uses and disclosures for which an authorization or opportunity to agree or object is not required §164.512(i)(1) - A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that: (i) Board approval of a waiver of authorization - The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either: (a) An Institutional Review Board (IRB); or (b) A privacy board that: (1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy	Uses and disclosures for research purposes	Inquire of management as to whether procedures to use PHI for research exist. Obtain and review procedures on use and disclosure to determine if the entity obtained authorization and/or waiver. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the entity: -

Section	Established Performance Criteria	Key Activity	Audit Procedures
	rights and related interests; (2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and (3) Does not have any member participating in a review of any project in which the member has a conflict of interest. (ii) Reviews preparatory to research - The covered entity obtains from the researcher representations that: (a) Uses or disclosures is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research; (b) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and (c) The protected health information for which use or access is sought is necessary for the research purposes. (iii) Research on decedent's information - The covered entity obtains from the researchers: (a) Representation that the use or disclosure sought is solely for research on the protected health information or decedents; (b) Documentation, at the request of the covered entity, of the death of such individuals; and (c) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes. Continued . . .		Obtains documentation that an alteration to a required authorization, or waiver of the authorization, has been approved by an IRB or privacy board. - Obtains from the researchers the required representations regarding reviews prepatory to research on decedents. Verify if the entity obtained the necessary authorization and/or waiver to conduct the research. Elements to consider should consist of performance criteria and include, but are not limited to: -Board approval of a waiver of authorization. - Whether the use or disclosure is solely to review PHI as necessary to prepare a research protocol. -Representation that the use or disclosure is solely for research on the PHI of decedents.
§164.512	§164.512 - Uses and disclosures for which an authorization or opportunity to agree or object is not required See above . . . §164.512(i)(2) - §164.512(i)(1) - Documentation of waiver approval - For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following: (i) Identification of IRB and/or date of action - A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved; (ii) Waiver criteria - A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria: (a) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements; (1) An adequate plan to protect the Identifiers from improper use and disclosure; (2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and (3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this	Uses and disclosures for research purposes	Inquire of management as to whether a process exists to determine what documentation of approval or waiver is needed to permit a use or disclosure. Obtain and review documentation of approval and evaluate the content in relation to the specified criteria of an alteration or waiver to determine if it contains all necessary information. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the documentation: -Includes identification and date of action. -Includes waiver criteria. -Includes PHI needed. -Requires review and approval procedures. -Requires signature. Obtain and review documentation

Section	Established Performance Criteria	Key Activity	Audit Procedures
	subpart; (b) The research could not practicably be conducted without the waiver or alteration; and (c) The research could not practicably be conducted without access to and use of the protected health information. (iii) Protected health information needed - A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board had determined, pursuant to paragraph (i)(2)(ii)(c) of this section; (iv) Review and approval procedures - A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows: (a) An IRB must follow the requirements of the Common Rule, including the normal review procedures or the expedited review procedures; (b) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(b)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedures in accordance with paragraph (i)(2)(iv)(C) of this section; (c) A privacy board may use an expedited review procedures if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and (v) Required signature - The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.		of approval and evaluate the content in relation to the specified criteria of an alteration or waiver to determine if it contains all necessary information. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the documentation: -Includes identification and date of action. -Includes waiver criteria. -Includes PHI needed. -Requires review and approval procedures. -Requires signature. Verify that the documentation of approval or waiver contains all the information necessary to permit a use or disclosure. Elements to consider include, but are not limited to: -A statement identifying IRB and the date on which the alteration or waiver of authorization was approved. -Whether IRB determined that the alteration or waiver satisfied certain criteria. -Whether IRB has determined the use or access of PHI. -Whether the alteration or waiver of authorization has been reviewed and approved. -The alteration or waiver was signed by the chair or other member of IRB.
§164.512	§164.512(a)(1) - A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies and is limited to the relevant requirements of such law. §164.512(a)(2) - A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.	Uses and disclosures required by law	Inquire of management as to whether the requirements to use or disclose PHI required by law are met. Obtain and review Notice of Privacy Practices and evaluate the content in relation to the specified criteria to determine if the entity identifies the disclosures required by law. Obtain and review policies and procedures and evaluate

Section	Established Performance Criteria	Key Activity	Audit Procedures
			the content in relation to the specified criteria for uses and disclosures required by law.
§164.512	§164.512(b)(1) - A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to: (i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority; (ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect. (iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated products or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include: (a) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations; (b) To track FDA-regulated products; (c) To enable product recalls, repairs, or replacement, or look back (including locating and notifying individuals who have received products that have been, withdrawn, or are the subject of look back); or (d) To conduct post marketing surveillance; (iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or (v) An employer, about an individual who is a member of the workforce of the employer, if: (a) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer: (1) To conduct an evaluation relating to medical surveillance of the workplace; or (2) To evaluate whether the individual has a work-related illness or injury; (b) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance; (c) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and (d) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer: (1) By giving a copy of the notice to	Uses and disclosures for public health activities	Inquire of management as to whether a process is in place specifying public health activities for which the entity may disclose PHI. Obtain and review formal or informal policies and evaluate the content in relation to the specified criteria on permitted uses and disclosures for public health activities. Obtain and review a sample of such uses/disclosures, to include (v) and determine whether all criteria were met. Auditors should refer to the established performance criteria to identify what subpart (v) includes.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	the individual at the time the health care is provided; or (2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.		
§164.512	§164.512(c)(1) - Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence: (i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; (ii) If the individual agrees to the disclosures; or (iii) To the extent the disclosure is expressly authorized by status or regulation and: (a) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or (b) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure. §164.512(c)(2) - A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if: (i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or (ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.	Disclosures about victims of abuse, neglect or domestic violence	Inquire of management as to whether disclosure about victims of abuse, neglect, or domestic violence are permitted. Inquire of management as to whether a process is in place to inform the individual that a disclosure has been or will be made. Obtain and review the policy and evaluate the content in relation to the specified criteria to determine whether the policy indicates when and in what instances the individual should be notified of disclosures. Obtain and review the policy and evaluate the content in relation to the specified criteria on permissible uses and disclosures.
§164.512	§164.512(d)(1) - A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of: (i) The health care system; (ii) Government benefit programs for which health information is relevant to beneficiary eligibility; (iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or (iv) Entities subject to civil rights laws for which health information is necessary for determining compliance. §164.512(d)(2) - For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the	Uses and disclosures for health oversight activities	Inquire of management as to whether PHI is disclosed to the appropriate health oversight agency. Obtain and review the policy on permissible uses and disclosures. Obtain a sample of disclosures made for this purpose and verify that criteria have been appropriately applied.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to: (i) The receipts of health care; (ii) A claim for public benefits related to health; or (iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services. §164.512(d)(3) - Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section. §164.512(d)(4) - If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.		
§164.512	§164.512(f) - A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable. (1) Pursuant to process and as otherwise required by law. A covered entity may disclose protected health information. (i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or (ii) In compliance with and as limited by the relevant requirements of: (a) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer; (b) A grand jury subpoena; or (c) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demands, or similar process authorized under law, provided that: (1) The information sought is relevant and material to a legitimate law enforcement inquiry; (2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (3) De-identified information could not reasonably be used. §164.512(f)(2) - Limited information for identification and location purposes: Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that: (i) The covered entity may disclose only the following information: (a) Name and address; (b) Date and place of birth; (c) Social security number; (d) ABO blood type and factor; (e)Type of injury; (f) Date and time of treatment; (g) Date and time of death, if applicable; and (h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos. (ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purpose of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records,	Disclosures for law enforcement purposes	Inquire of management as to whether conditions for disclosure of PHI to a law enforcement official are appropriate. Obtain and review policies and procedures related to disclosures of PHI to law enforcement officials. Obtain and review a sample of disclosures and the corresponding court orders, subpoenas, or discovery requests to law enforcement officials and determine if such disclosures are permitted. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure of PHI: -Is required by law. -Is in compliance with and as limited by the relevant requirements. Verify disclosure of PHI to a law enforcement official is permitted. Elements to consider include, but are not limited to: -Whether the law requires the reporting of certain types of physical injuries. -An administrative request, a grand jury subpoena, or a court order (warrant).

Section	Established Performance Criteria	Key Activity	Audit Procedures
	or typing, samples or analysis of blood fluids or tissue.		
§164.512	See above . . . §164.512(f)(3) - Victims of a crime - Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to a paragraph (b) or (c) of this section, if: (i) The individual agrees to the disclosures; or (ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that: (a) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim; (b) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (c) The disclosure is in the best interest of the individual as determined by the covered entity, in the exercise of professional judgment. §164.512(f)(4) - A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicious that such death may have resulted from criminal conduct. §164.512(f)(5) - Crime on premises - A covered entity may disclose to law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity. §164.512(f)(6) - Reporting crime in emergencies (i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to law enforcement official if such disclosure appears necessary to alert law enforcement to: (a) The commission and nature of a crime; (b) The location of such crime or of the victim(s) of such crime; and (g) The identity, description, and location of the perpetrator of such crime. (ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.	Disclosures for law enforcement purposes	Inquire of management as to whether the response to a law enforcement official's request is limited to information for identification and location purposes. Obtain and review responses to each category of disclosure in response to a law enforcement official's request to determine whether disclosure of such information is consistent with the requirements limiting disclosure to identification and location purposes. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure of PHI is limited to: - Identification and location purposes. Obtain and review a response to a law enforcement official's request to determine if disclosure of such information is limited to identification and location purposes. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure of PHI is limited to: - Identification and location purposes. Verify the information disclosed to a law enforcement official is limited to information for identification and location purposes. Elements to consider include, but are not limited to: -Whether information other than identification and location is disclosed.
§164.512	See above.	Disclosures for law enforcement purposes	Inquire of management as to whether conditions in which the entity may disclose PHI in response to

Section	Established Performance Criteria	Key Activity	Audit Procedures
			a law enforcement official's request are met prior to disclosure. Obtain and review a response to a law enforcement official's request to determine whether disclosure is permitted. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosures are made: -By the individual who agrees to the disclosure. -By the covered entity who was unable to obtain the individual's agreement because of incapacity or other emergency circumstances. Obtain and review a response to a law enforcement official's request to determine whether disclosure is permitted. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosures are made: -By the individual who agrees to the disclosure. -By the covered entity who was unable to obtain the individual's agreement because of incapacity or other emergency circumstances. Verify the disclosure of PHI is in response to a law enforcement official's request about a victim of crime and is permitted. Elements to consider include, but are not limited to: -Individual consent to disclose PHI. -Whether the entity exercised professional judgment.
§164.512	See above.	Disclosures for law enforcement purposes	Inquire of management as to whether a process is in place to determine when it is permitted to disclose PHI about an individual who

Section	Established Performance Criteria	Key Activity	Audit Procedures
			has died to a law enforcement official. Obtain and review disclosure about an individual who has died to determine the purpose. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the purpose of disclosure: - Was to alert law enforcement of the death of the individual, if the entity suspected that such death may have resulted from criminal conduct. - Was to alert law enforcement of criminal conduct that occurred on the premises of the entity. Verify that disclosure of PHI about an individual who has died to a law enforcement official is appropriate. Elements to consider include, but are not limited to: -Whether the entity exercised professional judgment. - Whether the entity believes in good faith that there was evidence of criminal conduct that occurred on its premises.
§164.512	See above.	Disclosures for law enforcement purposes	Inquire of management as to whether a process is in place to determine what information about a medical emergency is necessary to disclose to alert law enforcement. Obtain and review disclosures of medical emergencies to determine if it is necessary to alert law enforcement. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure: -Indicates the commission and nature of the crime. - Includes the location of the crime or the victim(s) of the

Section	Established Performance Criteria	Key Activity	Audit Procedures
			crime. -Includes the identity, description, and location of the perpetrator of the crime. Verify that disclosures to alert law enforcement appear necessary. Elements to consider include, but are not limited to: -Nature of crime is stated. -Location and victim(s) of the crime are identified. -Perpetrator of the crime is identified.
§164.512	§164.512(g)(1) - Coroners and medical examiners - A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs that duties or a coroner or medical examiner may use protected health information for the purposes described in this paragraph. §164.512(g)(2) - Funeral directors - A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.	Uses and disclosures about decedents	Inquire of management as to whether the process for disclosing PHI to a coroner or medical examiner is appropriate. Obtain and review disclosures about decedents to determine disclosures are appropriate. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the purpose of disclosure: -Is to identify a deceased person. -Is to determine the cause of death. -Is authorized by law. Verify disclosures about decedents are appropriate. Elements to consider include, but are not limited to: -Name of deceased person. -Cause of death. -Compliance with such law.
§164.512	§164.512(h) - A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissues for the purpose of facilitating organ, eye or tissue donation and transplantation.	Uses and disclosures for cadaveric organ, eye or tissue donation	Inquire of management as to whether the process for disclosing PHI to organ procurement organizations or other entities engaged in the procurement is appropriate. Obtain and review disclosures of PHI to organ procurement organization to determine the purpose of such disclosures. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure:

Section	Established Performance Criteria	Key Activity	Audit Procedures
			-Is for the purpose of facilitating organ, eye, or tissue donation and transplantation. Verify that disclosures of PHI to organ procurement organizations or other entities engaged in the procurement are for the purpose of facilitating organ, eye, or tissue donation and transplantation. Elements to consider include, but are not limited to: -The disclosures facilitate the process of organ, eye, or tissue donation and transplantation.
§164.512	§164.512(k)(1) - A covered entity may use or disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information: (a) Appropriate military command authorities; and (b) The purposes for which the protected health information may be used or disclosed. (ii) A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs. (iii) A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs. (iv) A covered entity may use or disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the Federal Register pursuant to paragraph (k)(1)(i) of this section. §164.512(k)(2) - A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act and implement authority. §164.512(k)(3) - A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C 3056, or to foreign heads of state or other persons authorized by 22 U.S.C 2709(a)(3), or to	Uses and disclosures for specialized government functions	Inquire of management as to whether a process is in place to determine for which government functions the entity is permitted disclose PHI. Obtain and review a list of uses and disclosures for government functions to determine the use and disclosure of PHI is appropriate. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure: -Is for an armed force personnel. -Is for a separated or discharged military service personnel. -Is for a veteran. -Is for a foreign military personnel. Verify disclosures of PHI are for appropriate government functions. Elements to consider include, but are not limited to: -Whether activities deemed necessary by appropriate military command authorities. -Whether the purpose is to determine the individual's eligibility for or entitlement to benefits under laws. -Whether it is for the appropriate foreign military

Section	Established Performance Criteria	Key Activity	Audit Procedures
	for the conduct of investigations authorized by 18 U.S.C 871 and 879. §164.512(k)(4) - A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes: (i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698; (ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or (iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.		personnel.
§164.512	See above. §164.512(k)(5) - Correctional institutions and other law enforcement custodial situations. (i) - A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for: (a) The provision of health care to such individuals; (b) The health and safety of such individual or other inmates; (c) The health and safety of the officers or employees of or others at the correctional institution; (d) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another; (e) Law enforcement on the premises of the correctional institution; and (f) The administration and maintenance of the safety, security, and good order of the correctional institution. (ii) A covered entity that is correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed. (iii) For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody. §164.512(k)(6) - Covered entities that are government programs providing public benefits (i) - A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined date system accessible to all such government agencies is required or expressly authorized by statute or regulation. (ii) - A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve in the same or similar populations and the disclosures of protected health information is necessary to coordinate the covered functions of such programs or to	Uses and disclosures for specialized government functions	Inquire of management as to whether a process is in place to determine why PHI is disclosed to authorized federal officials. Obtain and review disclosed PHI to determine that the purposes are appropriate and reasonable. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the purpose for the disclosure: -Is to conduct lawful intelligence. -Is for counter-intelligence. -Is for other national security activities authorized by the National Security Act. Verify disclosures of PHI are for activities authorized by the National Security Act. Elements to consider include, but are not limited to: -Whether activities are authorized by the National Security Act. -Whether lawful intelligence services are conducted.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	improve administration and management relating to the covered functions of such programs.		
§164.512	See above.	Uses and disclosures for specialized government functions	Inquire of management as to whether a process is in place to determine for what protective services the entity is permitted to disclose PHI. Obtain and review disclosed PHI to determine the disclosure is for protective services for authorized federal officials. Based on the complexity of the entity, elements to consider include, but are not limited to, whether disclosure of PHI is: -For the provision of protective services to the President. -For other authorized persons. -For the conduct of investigations authorized by 18 U.S.C 871 and 879. Verify disclosures of PHI are for protective services for authorized federal officials. Elements to consider include, but are not limited to: -Whether the protective services are for the President. -Authorization of persons. -Authorization of investigations.
§164.512	See above.	Uses and disclosures for specialized government functions	Inquire of management as to whether a process is in place to determine the purpose for disclosing PHI to the Department of State (DOS). Obtain and review PHI disclosed to DOS to determine the need to access such information. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure: -Is required to conduct security clearance pursuant to Executive Orders 10450 and 12698. -Is necessary to determine worldwide availability or availability for mandatory

Section	Established Performance Criteria	Key Activity	Audit Procedures
			service abroad under sections 101(a)(4) and 504 of the Foreign Service Act. -Is for a family to accompany a Foreign Service member abroad. Verify the need to access PHI is appropriate. Elements to consider include, but are not limited to: -Whether it is required for a security clearance. -Whether such information is required under the Foreign Service Act.
§164.512	See above.	Uses and disclosures for specialized government functions	Inquire of management as to whether a process is in place to determine if the disclosure of PHI to a correctional institution or law enforcement official is necessary. Obtain and review PHI disclosed to a correctional institution or law enforcement official and determine if the disclosure is necessary. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure is necessary for: -The provision of health care to such individuals. -The health and safety of such individual or other inmates. -The health and safety of the officers or employees of or at the correctional institution. -The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another. -Law enforcement on the premises of the correctional institution. -The administration and maintenance of the safety, security, and good order of the correctional institution.

Section	Established Performance Criteria	Key Activity	Audit Procedures
			Verify that disclosure of PHI to a law enforcement official is necessary. Elements to consider include, but are not limited to: -Whether the safety of such individual, other inmates, officers, employees, law enforcement, maintenance, and security is in danger.
§164.512	§164.512(l) - A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.	Disclosures for workers' compensation	Inquire of management as to whether a process is in place to determine the need to disclose PHI for the purpose of workers' compensation. Obtain and review PHI disclosed for the purpose of workers' compensation and determine if it is appropriate. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure: -Is authorized by and to the extent necessary to comply with laws relating to workers' compensation. -Provides benefits for work-related injuries, or illness, without regard to fault. Verify that disclosure of PHI for the purpose of workers' compensation is appropriate. Elements to consider include, but are not limited to: -Whether disclosure of such information complies with laws relating to workers' compensation. -Whether the disclosure provides benefits for work-related injuries, or illness, without regard to fault.
§164.514	§164.514 - Other requirements relating to uses and disclosures of protected health information §164.514(d)(2)(i) A covered entity must identify: (A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and (B) For each such person or class of persons, the category or categories of protected health information to which access is needed and	Minimum Necessary Uses of PHI	Inquire of management as to whether access to PHI is restricted. Obtain and review a sample of workforce members with access to PHI for their corresponding job title and

Section	Established Performance Criteria	Key Activity	Audit Procedures
	any conditions appropriate to such access. (ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.		description to determine appropriateness. Obtain and review policies and procedures and evaluate the content relative to the specified criteria for terminating access to PHI. Select a sample listing of former employees to confirm that access to PHI was terminated. NOTE: The rule requires that the class/job functions that need to use or disclose PHI be determined, and the information be limited to what is needed for that job classification.
§164.514	§164.514 - Other requirements relating to uses and disclosures of protected health information §164.514(d)(3)(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. (ii) For all other disclosures, a covered entity must: (A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and (B) Review requests for disclosure on an individual basis in accordance with such criteria. Exceptions can be found in §164.514(d)(3)(iii). §164.514(d)(5) For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.	Minimum Necessary Disclosures of PHI	Inquire of management as to whether policies and procedures are in place to limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of disclosure. Obtain and review policies and procedures related to minimum necessary and evaluate the content relative to the specified criteria. Obtain and review documentation related to the provision of minimum necessary access to PHI for individuals and evaluate the content relative to the specified criteria.
§164.514	§164.514 - Other requirements relating to uses and disclosures of protected health information §164.514(f) (1) A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of §164.508: (i) Demographic information relating to an individual; and (ii) Dates of health care provided to an individual. (2) (i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by §164.520(b)(1)(iii)(B) is included in the covered entity's notice; (ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications. (iii) The covered entity must make	Uses and Disclosures for Fundraising	Inquire of management as to whether the disclosure of PHI to a business associate or institutionally related foundation is limited to demographic information relating to an individual and the dates when health care was provided to an individual. Obtain and review policies and procedures and evaluate the content relative to the specified criteria to determine if disclosure of PHI to a

Section	Established Performance Criteria	Key Activity	Audit Procedures
	reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.		business associate or institutionally related foundation is limited to demographic information relating to an individual and the dates when health care was provided to an individual. Obtain and review an example of a disclosure for fundraising purposes to determine if the information is limited to demographic information relating to an individual and the dates when health care was provided to an individual. Obtain and review evidence that the policies and procedures are updated appropriately and conveyed to the workforce.
§164.514	§164.514 - Other requirements relating to uses and disclosures of protected health information §164.514(g) If a health plan receives protected heath information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.	Uses and Disclosures for Underwriting and Related Purposes	Inquire of management as to whether procedures are in place restricting the health plan's uses and/or disclosures of PHI for underwriting purposes for any other purpose except as may be required by law. Obtain and review health plan documents, including contract(s), and evaluate the content relative to the specified criteria to determine if PHI limitation for underwriting purposes is included. Obtain and review evidence that the policies and procedures are updated appropriately and conveyed to the workforce.
§164.514	§164.514 - Other requirements relating to uses and disclosures of protected health information §164.514(h)(1) Prior to any disclosure permitted by this subpart, a covered entity must: (i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and (ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation,	Verification Requirements	Inquire of management as to whether formal or informal policies and procedures are in place to verify the identity of individuals who request PHI. Obtain and review policies and procedures and evaluate the content relative to the specified criteria to determine if a

Section	Established Performance Criteria	Key Activity	Audit Procedures
	statement, or representation is a condition of the disclosure under this subpart. (2) (i) Conditions on disclosures. If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements. (A) The conditions in §164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met. (B) The documentation required by §164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with §164.512(i)(2)(i) and (v). (ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official: (A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status; (B) If the request is in writing, the request is on the appropriate government letterhead; or (C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official. (iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official: (A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; (B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority. (iv) Exercise of professional judgment. The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with §164.510 or acts on a good faith belief in making a disclosure in accordance with §164.512(j).		process is in place to verify the identity of individuals who request PHI. Obtain and review documentation of how the covered entity has verified the identity of several recent requestors of PHI. Obtain and review evidence that the policies and procedures are updated appropriately and conveyed to the workforce.
§164.514	§164.514(e)(1) A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section. Please refer to paragraphs (e)(2), (e)(3), and (e)(4) of the HIPAA Privacy Rule legislation.	Limited Data Sets and Data Use Agreements	Inquire of management as to whether data use agreements are in place between the covered entity and its limited data set recipients. Obtain and review policies and procedures and evaluate the content in relation to

Section	Established Performance Criteria	Key Activity	Audit Procedures
			the specified criteria to determine if data use agreements are in place between the covered entity and its limited data set recipients. Obtain and review an example data use agreement to determine if the agreements comply with the HIPAA standard. Obtain and review evidence that the policies and procedures are updated appropriately and conveyed to the workforce.
§164.514	§164.514(e)(4)(iii)(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful: (1) Discontinued disclosure of protected health information to the recipient; and (2) Reported the problem to the Secretary. (B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.	Limited Data Sets and Data Use Agreements	Inquire of management as to whether policies and procedures are in place to terminate data use agreements if the agreement is violated. Obtain and review policies and procedures and evaluate the content in relation to the specified criteria to determine if a process is in place to terminate data use agreements if the agreement is violated. Obtain and review evidence that the policies and procedures are updated appropriately and conveyed to the workforce.
§164.514	§164.514 - Other requirements relating to uses and disclosures of protected health information §164.514(c) A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that: (1) The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and (2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.	Re-Identification of PHI	Optional: A covered entity may re-identify PHI; however they are not required to. Inquire of management as to whether a process to re-identify PHI exists. Obtain and review policies and procedures and evaluate content in relation to the specified criteria to determine how PHI is re-identified. Obtain and review evidence that the policies and procedures are updated appropriately and conveyed to the workforce.

Section	Established Performance Criteria	Key Activity	Audit Procedures
§164.514	§164.514 - Other requirements relating to uses and disclosures of protected health information A covered entity may determine that health information is not individually identifiable health information only if: (1) A person with appropriate knowledge of any experience with generally accepted statistical scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify and individual who is a subject for the information; and (ii) Documents the methods and results of the analysis that justify such determination; or (2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current available data from the Bureau of the Census; (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.	De-Identification of PHI	Optional: A covered entity may de-identify PHI; however they are not required to. If a covered entity does de-identify PHI, inquire of management as to whether a process to de-identify PHI exists. Obtain and review policies and procedures and evaluate the content in relation to the specified criteria to determine a process in place to de-identify PHI. Verify that the policies and procedures are updated appropriately and conveyed to the workforce.
§164.520	§164.520 - Notice of Privacy Practices for PHI §164.520(a)(1) Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. §164.520(b)(1) The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph. (1) Required Elements. (i) Header. The notice must contain the following statement as a header or otherwise prominently displayed: ""THIS NOTICE	Notice of Privacy Practices	Inquire of management as to whether individuals are notified of the potential uses and disclosures of PHI by the covered entity. Obtain and review the notice of privacy practices and evaluate the content relative to the specified criteria given to individuals by the covered entity.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."" (ii) Uses and disclosures. The notice must contain: (A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations. (B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization. (C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in §160.202 of this subchapter. (D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law. (E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by §164.508(b)(5). (iii) Separate statements for certain uses or disclosures. If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that: (A) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual. (B) The covered entity may contact the individual to raise funds for the covered entity. (C) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.		Elements to consider include, but are not limited to: -That the notice of privacy practices specifically addresses how the individual's PHI may be used or to whom it may be disclosed. -That the notice of privacy practices specifically addresses what the individual's rights are. -That the notice of privacy practices specifically addresses the covered entity's legal duties with respect to PHI. Verify the privacy notices contain all the required elements specified by the HIPAA Privacy Standard.
§164.520	§164.520 - Notice of Privacy Practices for PHI §164.520(c)(1)(i) A health plan must provide notice: (A) no later than the compliance date for the health plan, to individuals then covered by the plan; (B) thereafter, at the time of enrollment, to individuals who are new enrollees; and (C) within 60 days of a material revision to the notice, to individuals then covered by the plan. (ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice. (iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents. (iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.	Provisions of Notice - Health Plans	Specific requirements for health plans: Inquire of management as to how the covered entity the notice to any person upon request. Obtain and review the formal or informal policies and procedures in place regarding the provision of the notice of privacy practices. For a selection of individuals, obtain and review the individuals' files for the past year to identify how frequently notices are provided and how individuals covered by the plan may obtain the notice of privacy practices.

Section	Established Performance Criteria	Key Activity	Audit Procedures
§164.520	§164.520 - Notice of Privacy Practices for PHI §164.520(c)(2) A covered health care provider that has a direct treatment relationship with an individual must: (i) Provide the notice: (A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or (B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation. (ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained; (iii) If the covered health care provider maintains a physical service delivery site: (A) Have the notice available at the service delivery site for individuals to request to take with them; and (B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice. (iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.	Provisions of Notice - Certain Covered Health Care Providers	Specific requirements for certain covered health care providers: Inquire of management as to how the covered entity the notice to any person upon request. Obtain and review the formal or informal policies and procedures in place regarding the provision of the notice of privacy practices. Obtain and review an example acknowledgement of receipt of the notice and an example of documentation showing a good faith effort was made when an acknowledgment could not be obtained. For a selection of individuals who were new patients/new individuals, obtain and review documentation to determine if the initial date of service corresponded with the date of the notice of privacy practices was received If the dates do not correspond, determine if the initial service was an emergency situation or if there was another means or explanation.
§164.520	§164.520 - Notice of Privacy Practices for PHI §164.520(c)(3) A covered entity that maintains a website that provides information about the covered entity's customer services or benefits must prominently post its notice on the website and make the notice available electronically through the website. (ii) A covered entity may provide the notice required by this section to an individual by email, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the email transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when made in accordance with paragraph (c)(1) or (2) of this section. (iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice. (iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the	Provisions of Notice - Electronic Notice	Specific requirements for electronic notice: If the covered entity provides electronic notice, obtain and review the policies and procedures regarding the provision of the notice of privacy practices by email and the process by which an individual can withdraw their request for receipt of electronic notice. If the covered entity maintains a website, observe the website to determine if the notice of privacy practices is prominently displayed and available. If the covered entity provides the notice of privacy practices by email, obtain and review

Section	Established Performance Criteria	Key Activity	Audit Procedures
	notice from a covered entity upon request.		an example of an agreement to receive the notice via e-mail.
§164.520	§164.520 - Notice of Privacy Practices for PHI §164.520(c)(4) Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that: (1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement. (2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity: (i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies; (ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and (iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement. (3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.	Joint Notice by Separate Covered Entities	Covered entities that participate in organized health care arrangements: Inquire of management as to whether a joint notice of privacy practices meets the minimum requirements set forth by the HIPAA Privacy Standards. Obtain and review the joint notice of privacy practices to determine whether right to it meets the minimum requirements specified by the HIPAA Privacy Standards.
§164.520	§164.520(e) A covered entity must document compliance with the notice requirements, as required by §164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.	Documentation	Inquire of management as to whether the documentation of privacy practices must be maintained in electronic or written form and retained for a period of six years. Obtain and review documentation to determine if (1) the notice of privacy practices, and (2) acknowledgements for health care providers with direct patient relationships are maintained in electronic or written form and retained for a period of six years.
§164.522	§164.522 - Rights to Request Privacy Protection for PHI §164.522(b)(1)(i) A covered entity must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health	Confidential Communications Requirements	Inquire of management as to whether the covered entity permits individuals to request alternative means

Section	Established Performance Criteria	Key Activity	Audit Procedures
	information from the covered health care provider by alternative means or at alternative locations. (ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.		or alternative locations to receive communications of PHI. Obtain and review formal or informal policies and procedures describing how an individual may request to receive communications of PHI by alternative means and at alternative locations.
§164.522	§164.522(a)(2) A covered entity may terminate its agreement to a restriction, if : (i) the individual agrees to or requests the termination in writing; (ii) the individual orally agrees to the termination and the oral agreement is documented; or (iii) the covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.	Terminating a Restriction	Inquire of management as to whether a process is in place to terminate restrictions of the use and/or disclosure of PHI. Obtain and review policies and procedures around terminating restrictions of use and/or disclosure of PHI. Obtain and review an example of a documented terminated restriction to determine that the terminated restrictions are being formally documented and adhered to. If documentation does not exist, may need to rely on inquiry only.
§164.522	§164.522(a)(3) A covered entity that agrees to a restriction must document the restriction in accordance with §164.530(j).	Documentation	Inquire of management as to whether documentation of restrictions is maintained in electronic or written form and retained for a period of six years. Obtain and review policies and procedures to determine if a process is outlined for documenting restriction requests and maintaining those documented restrictions for six years. Obtain and review documentation to determine if documentation of restrictions is maintained in electronic or written form and retained for a period of six years. If documentation does not exist, may need to rely on inquiry only.
§164.522	§164.522 - Rights to Request Privacy Protection for PHI §164.522(a)(1)(i) A covered entity must permit an individual to	Right of an Individual to	Inquire of management as to whether the covered

Section	Established Performance Criteria	Key Activity	Audit Procedures
	request that the covered entity restrict: (A) uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and (B) disclosures permitted under §164.510(b). (ii) A covered entity is not required to agree to a restriction. (iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual. (iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information. (v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§164.502(a)(2)(ii), 164.510(a) or 164.512.	Request Restriction of Uses and Disclosures	entity has a process in place to permit an individual to request that the entity restrict uses or disclosures of PHI. Obtain and review policies and procedures to determine if a process is in place to allow an individual to request that the covered entity restrict the use and/or disclosure of PHI.
§164.524	§164.524 - Access of Individuals to PHI §164.524(a)(1) Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to review and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set. §164.524(b)(1) The covered entity must permit an individual to request access to review or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement. §164.524(b)(3) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to review or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access. §164.524(b)(4) If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of: (i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual; (ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and (iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section. §164.524(c)(3) If the covered entity does not maintain the protected health	Right to access	Inquire of management as to how an individual can access PHI. Obtain and review formal or informal policies and procedures to determine a if a process is in place for individuals to access PHI. Obtain and review the notice of privacy practices to identify if an individual's right to access in timely manner is outlined in the notice. Determine whether fee charged meets criteria.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.		
§164.524	§164.524 - Access of Individuals to PHI §164.524(a)(4) If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section. §164.524(d)(4) If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial, to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.	Review of denial of access	Inquire of management as to whether a process to facilitate review of denial of access is in place. Obtain or inquire about the formal or informal process to determine whether it meets the requirements of the established criteria. Determine if the entity has a process in place for an individual to request and receive a review of a denial of access by a licensed health care professional who did not participate in the original decision to deny the individual's request for access.
§164.524	§164.524(a)(2) A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances. (i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section (see selected area). (ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate. (iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research. (iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law. (v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of	Unreviewable ground for denial	Inquire of management as to whether the unreviewable denied requests for access are properly documented. Obtain and review a list of unreviewable denials of access. Verify that the circumstances that trigger unreviewable grounds for denial apply to the denied access.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	confidentiality and the access requested would be reasonably likely to reveal the source of the information.		
§164.524	§164.524(a)(3) A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances: (i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or (iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person. §164.524(d)(2) The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain: (i) The basis for the denial; (ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and (iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in §164.530(d) or to the Secretary pursuant to the procedures in §160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).	Reviewable grounds for denial	Inquire of management as to whether the policies and procedures are in place to have the denial of access reviewed. Obtain and review policies and procedures to determine a process in place to allow an individual to request a review of the denial of access.
§164.524	§164.524(e) A covered entity must document the following and retain the documentation as required by §164.530(j): (1) the designated record sets that are subject to access by individuals; and (2) the titles of the persons or offices responsible for receiving and processing requests for access by individuals.	Documentation	Inquire of management as to whether a process of document retention for amendments to PHI is in place. Obtain and review policies and procedures to determine if a person or office is specified to process requests for amendments by individuals. Obtain and review the process to determine proper documentation is maintained and retained for a period of six years.
§164.526	§164.526(a)(1) An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated	Right to Amend	Inquire of management as to whether a policy exists regarding an individual's right to amend their PHI in

Section	Established Performance Criteria	Key Activity	Audit Procedures
	record set.		a designated record set. Obtain and review authoritative documentation to determine the individual's right to amend PHI in a designated record set is included. Verify the process allows the individual the right to amend protected health information in a designated health record set.
§164.526	§164.526(a)(2) A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request: (i) was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment; (ii) is not part of the designated record set; (iii) would not be available for reviewing under §164.524; or (iv) is accurate and complete.	Denying the Amendment	Inquire of management as to whether grounds for denying requests for amendment are documented. Obtain and review documentation that outlines a list of circumstances by which the entity has grounds for denial of amendment. Verify grounds for denying request for amendment is appropriate.
§164.526	§164.526(c) If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements. (1) The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment. (2) In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section. (3) The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to: (i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and (ii) persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.	Accepting the Amendment	Inquire of management as to whether requirements the entity must comply with are documented if a request for amendment is accepted. For a selection of requests for amendments, obtain and inspect a list of requirements to determine if the entity is in compliance with these requirements. Verify the entity is in compliance with all requirements if the request for amendment is accepted.
§164.526	§164.526(d) If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the requirements set forth in the HIPAA Privacy Standards: Provide the individual with a timely written denial.	Denying the Amendment	Inquire of management as to whether the requirements the entity must comply with are

Section	Established Performance Criteria	Key Activity	Audit Procedures
	Permit the individual to submit a written statement of disagreement with instructions on how to submit the statement and inform the individual of complaint procedures (see the HIPAA Privacy Protocol for §164.530). Prepare a written rebuttal if the individual submits statement of disagreement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement. Have a recordkeeping system. (4) Recordkeeping: The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set. Future disclosures of the individual's PHI must be made of the denial of amendment and statements of disagreement, if applicable. (5)Future disclosures: (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates. (ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section. (iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.		documented if a request for amendment is denied. Obtain and inspect a list of requirements to determine if the entity is in compliance with all of these requirements. Verify if the entity is in compliance with the requirements by which the entity denies the request for amendment.
§164.528	§164.528(a) Right to an accounting of disclosures of protected health information. (1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years to the date on which the accounting is requested, except for disclosures: (i) To carry out treatment, payment and health care operations as provided in §164.506; (ii) To individuals of protected health information about them as provided in §164.502; (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in §164.502; (iv) Pursuant to an authorization as provided in §164.508; (v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in §164.510; (vi) For national security or intelligence purposes as provided in §164.512(k)(2); (vii) To correctional institutions or law enforcement officials as provided in §164.512(k)(5); (viii) As part of a limited data set in	Right to an Accounting of Disclosures of PHI	Inquire of management as to whether policies and procedures exist for an accounting of disclosures of PHI. Obtain and review policies and procedures in place to determine an accounting of disclosures is made.

Section	Established Performance Criteria	Key Activity	Audit Procedures
	accordance with §164.514(e); or (ix) That occurred prior to the compliance data for the covered entity. The policies and procedures allow for an individual to request an accounting of disclosures of their PHI in the prior six years, or less, of the request. The policies and procedures prevent an accounting of disclosures being provided to an individual if it will impede law enforcement or health agency's activities so long as the request is in writing. If the request is made orally, the covered entity must document the statement, temporarily suspend the individual's right to the accounting of disclosures and limit the suspension for no more than 30 days unless the statement is received in writing during that time.		
§164.528	§164.528(b) The covered entity must provide the individual with a written accounting that meets the following requirements. The content must include disclosures made six years prior to the request (or shorter if the individual specifies), including disclosures made to or by business associates of the covered entity. The content must include the date; name and address of the entity provided the PHI; a description of the PHI disclosed and a brief statement of the purpose of the disclosure; and why the information was disclosed. If multiple disclosures have been made by the covered entity to the same person or entity for a single purpose, then the information listed above must be included for the first disclosure along with the number of disclosures made within the requested accounting period and the date of the last disclosure. If the covered entity made disclosure for research purposes to 50 or more individuals, then the name of the research activity; a description of the research activity; the type of PHI disclosed; the date or period of time the PHI was disclosed along with the last date it was disclosed; the name, address, and phone number of the research sponsor; and a statement that the PHI of the individual may or may not have been disclosed for a particular research activity must be included. The covered entity must assist the individual in contacting the research sponsor and researcher at the request of the individual.	Content of the Accounting	Inquire of management as to whether the content of the accounting of disclosures must meets the minimum requirements set forth in the HIPAA Privacy Standards. Obtain and review policies and procedures to determine if the covered entity meets the minimum requirements of content for accounting disclosures.
§164.528	§164.528(c)(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows. The policies and procedures specify the accounting of disclosures of PHI be provided no later than 60 days from the date of request by the individual. The policies and procedures specify that, if the covered entity cannot provide the accounting of disclosures, then the time can be extended no longer than 30 days so long as an explanation is provided in writing. The policies and procedures specify that they provide the individual with their first accounting of disclosures free of charge for any 12 month period. A reasonable, cost-based fee may be imposed on the same individual with a 12 month period so long as the covered entity informs the individual in advance of the fee and provides the individual an opportunity to withdraw or modify the request to avoid the fee.	Provision of the Accounting	Inquire of management as to whether policies and procedures exist to provide the individual with the requested accounting of PHI. Obtain and review policies and procedures to determine if a process exists to provide the individual with the requested accounting of PHI.

Section	Established Performance Criteria	Key Activity	Audit Procedures
§164.528	§164.528(d) A covered entity must document the following and retain the documentation as required by §164.530(j): (1) the information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section; (2) the written accounting that is provided to the individual under this section; and (3) the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.	Documentation	Inquire of management as to how accounting of disclosures is documented and retained. Obtain and review policies and procedures to determine if accounting of disclosures is documented and retained. Obtain and review an example of an accounting of disclosures of PHI to determine if the documentation complies with the HIPAA Privacy Standards. Obtain of and review documentation of all accounting of disclosures made within the past year to determine if the documentation complies with HIPAA Privacy Standards.
§164.530	§164.530 - Administrative Requirements §164.530(b)(1) A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity. §164.530(b)(2)(i)(A) Training must be provided to each member of the covered entity's workforce by no later than the compliance date for the covered entity; (B) thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and (C) to each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart within a reasonable amount of time.	Training	Inquire of management as to whether training is provided to the entity's work force on HIPAA Privacy Standards. Obtain and review documentation to determine if a training process is in place for HIPAA privacy standards. Obtain and review documentation to determine if a monitoring process is in place to help ensure all members of the workforce receive training on HIPAA privacy standards as mandated by §164.530(b)(1) and §164.530(b)(2)(i). For a selection of new hires within the audit period, obtain and review documentation showing training on HIPAA privacy compliance has been completed.
§164.530	§164.530 - Administrative Requirements §164.530(d)(1) A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the	Complaints to the Covered Entity	Inquire of management as to whether formal or informal policies and procedures exist for receiving and processing

Section	Established Performance Criteria	Key Activity	Audit Procedures
	requirements of this subpart or subpart D of this part.		complaints over the entity's privacy practices. Obtain and review formal or informal policies and procedures to determine how complaints are received, processed, and documented. From a population of complaints received within the audit period, obtain and review documentation of each complaint.
§164.530	§164.530 - Administrative Requirements §164.530(e)(1) A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart.	Sanctions	Inquire of management as to whether sanctions are in place against members of the covered entity's workforce who fail to comply with the privacy policies and procedures. Obtain and review formal or informal policies and procedures to determine if sanctions are identified/described in the event members of the workforce do not comply with the entity's privacy practices. From a population of instances of individual/employee non-compliance within the audit period, obtain and review documentation to determine whether appropriate sanctions were applied. Obtain and review evidence that the policies and procedures are updated and conveyed to the workforce.
§164.530	§164.530 - Administrative Requirements §164.530(i)(1) A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. §164.530(i)(2)(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart.	Policies and Procedures	Inquire of management as to whether policies and procedures with respect to PHI are in place that are designed to comply with the standards, implementation specifications, and other requirements of the HIPAA Privacy Standards.
§164.530	§164.530 - Administrative Requirements §164.530(c)(2)(i) A covered entity must reasonably safeguard protected health	Administrative, Technical and	Inquire of management as to whether administrative,

Section	Established Performance Criteria	Key Activity	Audit Procedures
	information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. §164.530(c)(2)(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.	Physical Safeguards	technical, and physical safeguards are in place to protect all PHI. Please refer to the HIPAA Security Compliance protocols for details on how to test the administrative, technical, and physical safeguards in place over EPHI. Obtain and review procedures and policies and evaluate the content to determine if administrative, technical, and physical safeguards are in place to protect all PHI (e.g., electronic PHI, written PHI, rules about speaking about PHI). Observe and verify whether the safeguards in place are appropriate.
§164.530	§164.530 - Administrative Requirements §164.530(f)(1) A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.	Mitigation	Inquire of management as to whether the covered entity mitigates any harmful effect that is known to the covered entity of a use or disclosure of PHI by the covered entity or its business associates, in violation of its policies and procedures . Obtain and review policies and procedures in place to determine if the covered entity mitigates any harmful effect that is known to the covered entity of a use or disclosure of PHI by the covered entity or its business associates, in violation of its policies and procedures. Obtain and review documentation to determine if a monitoring process is in place to help management ensure corrective action/mitigation plans are developed pursuant to relevant policies or procedures. From a population of instances of non-compliance within the audit

Section	Established Performance Criteria	Key Activity	Audit Procedures
			period, obtain and review documentation to determine whether corrective action/mitigation plans were developed and applied pursuant to relevant policies or procedures. Obtain and review evidence that the policies and procedures are updated appropriately and conveyed to the workforce.
§164.530	§164.530 - Administrative Requirements §164.530(g)(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and (2) must refrain from intimidation and retaliation as provided in §160.316.	Refraining from Intimidating or Retaliatory Acts	Inquire of management as to whether policies and procedures exist preventing intimidating or retaliatory actions against any individual for the exercise by the individual of any right established, or for participation in any process provided, for filing complaints against the covered entity. Obtain and review policies and procedures in place and evaluate the content relative to the specified criteria to determine if anti-intimidation and anti-retaliatory standards exist. Obtain and review evidence that the policies and procedures are updated appropriately and conveyed to the workforce.

HIPAA Breach Notification Rule

Section	Established Performance Criteria	Key Activity	Audit Procedures
§164.402	§164.402 - Definitions Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	Risk Assessment of Breach	Inquire of management as to whether a risk assessment process exists to determine significant harm in a breach.
§164.404	§164.404 - Notice to Individuals §164.404 (a) A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	Notification to Individuals	Inquire of management as to whether a process exists for notifying individuals within the required time period. Obtain and review key documents that outline the process for notifying individuals of breaches.
§164.404	§164.404 - Notice to Individuals 164.404(b) Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.	Timeliness of Notification	Inquire of management as to whether a process exists for notifying individuals within the required time period. Obtain and review key documents that outline the process for notifying individuals of breaches. Verify, if any breaches have occurred, that individuals were notified within 60 days.
§164.404	§164.404 - Notice to Individuals (d) The notification required by paragraph (a) shall be provided in the following form: (1) (i)Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available. (ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available. (2) Substitute notice. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a	Methods of Individual Notification	Inquire of management as to whether a process exists for notifying an individual or an individual's next of kin of a breach. Obtain and review formal or informal documentation that provide the process and method for notifying individuals of a breach and compare it to established performance criteria. Inquire of management of the process for identifying an individual's contact information or next of kin and the process for follow-up when there is

Section	Established Performance Criteria	Key Activity	Audit Procedures
	substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii). (i) In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means. (ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach. (3) In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.		insufficient contact information. Obtain and review formal documentation that identifies the methods for providing notification where contact information is insufficient or out-of-date and compare to established performance criteria.
§164.404	§164.404 (c)(1)Elements of the notification required by paragraph (a) of this section shall include to the extent possible: (A)a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) any steps the individual should take to protect themselves from potential harm resulting from the breach; (D) a brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an email address, website, or postal address. (2) The notification required by paragraph (a) of this section shall be written in plain language.	Content of Notification	Inquire of management to determine if there is a standard template or form letter for breach notification. Verify that, if any breaches have occurred, the notification to the individuals included the required elements of this section.
§164.406	§164.406(a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b)Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery	Notification to the media	Inquire of management as to whether a process exists for notifying media outlets for breaches of more than 500 individuals' PHI and compare it to established performance criteria. Verify if any breaches of

Section	Established Performance Criteria	Key Activity	Audit Procedures
	of a breach. (c) The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c)		unsecured PHI have involved more than 500 individuals and have required notification of media outlets.
§164.408	§164.408(a) A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary (b) For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site. (c) For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	Notification to the Secretary	Inquire of management as to whether there have been any breaches of unsecured PHI and verify that the Secretary was notified. Verify if any breaches of unsecured PHI have involved more than 500 individuals and have required contemporaneous notification to the Secretary. Verify if any breaches of unsecured PHI have involved less than 500 individuals and have required annual notification through the HHS website.
§164.410	§164.410(a) (1)A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach (2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency) (b) Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach. (c) (1)The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach. (2) A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Notification by a business associate	Inquire of management as to whether there have been any breaches of unsecured PHI for a business associate and verify that the covered entity was notified. Obtain the standard business associate agreement to verify that the breach and notification elements are included in the agreement.

Section	Established Performance Criteria	Key Activity	Audit Procedures
§164.412	§164.412 If a law enforcement official states to a §164.412 If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or...	Law enforcement delay	Inquire of management as to how notifications are delayed in case of law enforcement requests. Obtain and review documentation of the process to delay notifications in case of law enforcement requests.
§164.414	§164.414 - Administrative requirements and burden of proof In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402. See §164.530 for definition of breach.	Burden of Proof	Inquire of management as to whether a risk assessment process exists to determine significant harm in a breach. Inquire of management as to whether a process exists to ensure that all notifications were made as required or that the impermissible use or disclosure did not constitute a breach. Obtain and review documentation of uses or disclosures that were not determined to be breaches and the corresponding risk assessment documentation.