Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

OCR HIPAA Audit Protocol – Redline of Prior Version and April 2016 Update

HIPAA Compliance Area	Key Activity	Established Performance Criteria	Audit Procedures	Implementation Specification
Security	General Requirements	§164.306(a): Covered entities and business associates must do the following: (1)Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2)Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3)Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.	General requirements, not a part of an audit inquiry: The Security Rule compliance practices of covered entities and business associates will be audited against the specific requirements described in the following sections. These specific requirements will be assessed based on the overarching principles set forth in the general requirements that pertain to all the security standards. Specifically, does the covered entity or business associate: 1. Ensure confidentiality, integrity and availability of ePHI? 2. Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI? 3. Protect against reasonably anticipated uses or disclosures of ePHI that are not permitted or required by the Privacy Rule? 4. Ensure compliance with Security Rule by its workforce?	
Security	Flexibility of approach	§164.306(b): Flexibility of approach. (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding	To determine which security measures the entity implements, the covered entity or business associate should take into account the following factors. 1. Its size, complexity, and capabilities. 2. Its technical infrastructure, hardware, and software security capabilities. 3. The costs of security measures.	

		which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.	4. The probability and criticality of potential risks to ePHI. Use these general requirements and factors when assessing an entity's compliance with the specific requirements of the Security Rule.	
Security	Security Management Process	§164.308(a): A covered entity or business associate must in accordance with 164.306: (1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.	Does the entity have written policies and procedures in place to prevent, detect, contain and correct security violations? Does the entity prevent, detect, contain and correction security violations? Obtain and review policies and procedures related to security violations. Evaluate the content relative to the specified performance criteria for countermeasures or safeguards implemented to prevent, detect, contain and correct security violations. Obtain and review documentation demonstrating that policies and procedures have been implemented to prevent, detect, contain, correct security violations. Evaluate and determine if the process used is in accordance with related policies and procedures. Obtain and review documentation of security violations and remediation actions. Evaluate and determine if security violations where	Required

			handled in accordance with the related policies and procedures; safeguards or countermeasures to prevent violations from occurring; identify and characterize violations as they happen; limit the extent of any damages caused by violations; have corrective action plan in place to manage risk.	
Security	Evaluation	§164.308(a)(8): 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 a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	Does the entity have policies and procedures in place to perform periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes or newly recognized risk affecting the security of ePHI? Does the entity perform periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes or newly recognized risk affecting the security of ePHI? Obtain and review documentation of policies and procedures related to technical and nontechnical evaluation. Determine if such policies and procedures identifies how the evaluation of findings, remediation options and recommendations, and remediation decisions are documented; specifies that evaluations will be repeated on a periodic basis and/or when environmental and operations changes are made and/or newly recognized risk affects the security of ePHI; and identifies the frequency of when to evaluate and update the current policy and procedures.	Required

			Elements to review may include but are not limited to: • Workforce members' roles and responsibilities in the technical and nontechnical evaluation • Management involvement in the process and approval of technical and nontechnical evaluation • Coordination of technical and nontechnical evaluation among departments • Specification of how technical and nontechnical evaluation will be conducted • How technical and nontechnical evaluation findings will be addressed Obtain and review documentation demonstrating periodic technical and non-technical evaluations. Evaluate and determine if the such evaluation appropriately evaluates ePHI security measures; addresses evaluation findings associated with noncompliant security measures; identifies and measures risks associated with noncompliant security measures; and that evaluation findings are reviewed and certified by appropriate management. Obtain and review documentation of procedures for technology change control/management and documentation of major technology changes which affected the security of ePHI. Obtain and review documentation of plans related to risk management or mitigation efforts in response to evaluations conducted due to a major technology change which affected the security of ePHI. Evaluate and determine if the identified risks associated with	

			noncompliant security measures are addressed in a plan related to risk management or mitigation efforts.	
Security	~~Conduct~~ Security Management Process -- Risk ~~Assessment~~Analysis	~~§164.308(a)(1):~~ ~~Security Management Process~~ §164.308(a)(1)(ii)(~~a~~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 or business associate.	~~Inquire of management as to whether formal or informal~~Does the entity have policies ~~or practices exist~~and procedures in place to conduct an accurate and thorough assessment of the 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~~all the electronic protected health information (ePHI) it creates, receives, maintains, or transmits? Has the entity conducted an accurate and thorough assessment of the 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~~to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits? Determine how the entity has implemented the requirements. Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in	Required

			risk analysis and how frequently the risk analysis will be reviewed and updated. Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. Evaluate and determine whether the risk analysis or other documentation contains: • A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI • Details of identified threats and vulnerabilities • Assessment of current security measures • Impact and likelihood analysis • Risk rating Obtain and review documentation regarding the written risk analysis or other documentation that immediately preceded the current risk analysis or other record, if any. Evaluate and determine if the risk analysis has been reviewed and updated on a periodic basis, in response to 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~~environment and/or operations, security incidents, or occurrence of a significant event. If there is no prior risk analysis or other record, obtain and review the two (2) most	

			recent written updates to the risk analysis or other record, if any. If the original written risk analysis or other records have not been updated since they were originally conducted and/or drafted, obtain and review an explanation as to the reason why.	
~~Security~~	~~Acquire IT Systems and Services~~	~~§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.~~	~~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~~

~~Security~~	~~Develop and Deploy the Information System Activity Review Process~~	~~§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.~~	~~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 a periodic basis.~~	~~Required~~
Security	~~Implement a~~ Security Management Process ~~--~~ Risk Management ~~Program~~	~~§164.308(a)(1):~~ ~~Security Management Process~~ §164.308(a)(1)(ii)(~~b~~B)~~–~~: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	~~Inquire of management as to whether current security measures are sufficient to~~ Does the entity have policies and procedures in place regarding a risk management process 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~~ level?	Required

			Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level? Obtain and review policies and procedure related to risk management. Evaluate and determine if the documents identify how risk will be managed, what is considered an acceptable level of risk based on management approval, the frequency of reviewing ongoing risks, and identify workforce members' roles in the risk management process. Obtain and review documentation demonstrating the security measures implemented and/or in the process of being implemented as a result of the risk analysis or assessment. Evaluate and determine whether the implemented security measures appropriately respond to the threats and vulnerabilities identified in the risk analysis according to the risk rating and that such security measures are sufficient to mitigate or remediate identified risks to an acceptable level.	
~~Security~~	~~Select a Security Official To Be Assigned Responsibility for HIPAA Security~~	~~§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.~~	~~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~~	~~Required~~

			~~Security Official have been clearly defined.~~	
Security	~~Assign and Document the Individual's Responsibility~~Security Management Process – Sanction Policy	§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~~1)(ii)(C): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	~~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~~Does the entity have policies and procedures in place regarding sanctions to apply to workforce members who fail to comply with the entity's security policies and procedures? Does the entity apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures? Obtain and review documentation of the sanction policies and procedures (which could be an aspect of a larger code of conduct). Evaluate if they contain a	Required

			reasonable and appropriate process to sanction workforce members for failures to comply with the entity's security policies and procedures. Elements to review may include but are not limited to: • Personnel involved in the sanction process • Required steps and time period • Notification steps • Reason for the sanction • Identification of the sanctions applied to compliance failures • Documentation of the sanction outcome Obtain and review documentation demonstrating sanctions against workforce members. Evaluate and determine whether appropriate sanctions were applied for workforce members that failed to comply with security policies and procedures.	
Security	~~Implement Procedures for Authorization and/or Supervision~~Security Management Process --Information System Activity Review	§164.308(a)(~~3~~1)(ii)(~~A~~D): ~~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~~to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	~~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~~	~~Addressable~~Required

			~~specification and their rationale for doing so~~Does the entity have policies and procedures in place regarding the regular review of information system activity? Does the entity regularly review records of information system activity? Obtain and review policies and procedures related to reviewing records of information system activities. Evaluate and determine if reasonable and appropriate processes are in place to review records of information system activities, such as audit logs, access reports, and security incident tracking reports. Elements to review may include but are not limited to: • How often a review is performed • How reviews are documented • Workforce members' roles and responsibilities in the regular records of the information systems activities • Types of activities which may require further investigation Obtain and review documentation demonstrating the records of information system activities that were reviewed such as audit logs, access reports, and security incident tracking reports. Evaluate and determine if information system records were reviewed in a timely manner and that the review was conducted and certified by appropriate personnel. Obtain and review documentation demonstrating the capabilities of the	

			information system activity logs. Evaluate and determine whether key information systems have the capabilities to generate activity records; and, if so, are the capabilities turned on and records generated.	
Security	Assigned Security Responsibility	§164.308(a)(2): Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Does the entity have policies and procedures in place regarding the establishment of a security official? Has the entity identified the security official responsible for the development and implementation of the policies and procedures required by this subpart? Obtain and review documentation of the assigned Security Official(s) responsibilities (e.g., job description) and that a natural person has been named to act as the Security Official and/or other individuals have been assigned with other security duties. Evaluate and determine whether the organization has assigned responsibility for compliance with the Security Rule to a Security Official who oversees the development and implementation (to include monitoring and communication) of security policies and procedures and/or assigned other individuals with other security duties; and the responsibilities of the Security Official(s) have been clearly defined.	Required
Security	~~Establish Clear Job Description and Responsibilities~~Workforce Security	§164.308(a)(3) (i): ~~Workforce Security -~~ Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected	~~Inquire of management as to whether a formal document is in place identifying~~Does the entity have policies and procedures in place to ensure all members of its workforce have appropriate access to ePHI?	~~Addressable~~R

		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.	Does the entity ensure all members of its workforce have appropriate access to ePHI? Obtain and review the policies and procedures that ensure all members of its workforce only have access to ePHI that is required for each workforce member to do his or her job. Elements to review may include but are not limited to: • That different levels of access to information systems ~~that houses ePHI. Obtain and review formal documentation and evaluate the content in relation to the specified criteria to determine that levels of access are granted based on business need. Obtain and review evidence that the formal documentation establishing levels of access is~~are appropriately approved and communicated~~. Obtain and review relevant job descriptions and evaluate the content in relation to the specified performance criteria~~ • Ensuring that the workforce operates at privilege levels no higher than necessary to accomplish required job duties Obtain and review documentation demonstrating access granted to workforce members and their job descriptions. Evaluate and determine that ~~roles and responsibilities are defined and~~access granted to workforce members correlate with their job ~~function. If the covered entity~~	

			~~has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not~~functions/duties. Obtain and review documentation demonstrating that management reviews workforce members' access to ~~fully implement this specification and their rationale for doing so.~~ information systems that contain ePHI to determine if access is appropriate. Evaluate and determine if workforce members' access to information systems that contain ePHI is certified and approved by appropriate management.	
Security	~~Establish Criteria~~Workforce security -- Authorization and ~~Procedures for Hiring and Assigning Tasks~~/or Supervision	§164.308(a)(3) (ii)(A): ~~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~~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.	~~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~~Does the entity have policies and procedures in place regarding the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed? Does the entity authorize and/or supervise workforce member who work with ePHI or in locations where it might be accessed? Obtain and review policies and procedures related to the authorization and/or supervision of workforce members. Evaluate the content in relation to the specified ~~criteria.~~ performance criteria and determine that	Addressable

			appropriate authorization and/or supervision of workforce members who work with ePHI or in a location where it might be accessed is incorporated in the process. Obtain and review documentation regarding how requests for information systems that contain ePHI and access to ePHI are processed. Evaluate and determine if appropriate authorization and/or supervision for granting access to information systems that contain ePHI is incorporated in the process and is in accordance with related policies and procedures. Elements to review may include but are not limited to: • Identification of who has the authorization and/or supervisory permission to approve access to information systems and/or locations where ePHI may be accessed • How access requests to information systems are submitted • How access to the information systems is granted • How requests to access ePHI are submitted • How access to ePHI is granted • How authorization and/or supervisory approvals are verified • How a workforce member's level of access to ePHI is verified 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~~how access requests to locations where ePHI might be accessed are processed. Evaluate and determine if appropriate authorization for granting access to locations where ePHI might be accessed is incorporated in the process and is in accordance with related policies and procedures. Elements to review may include but are not limited to: • How access requests to locations are submitted • How access requests to locations are granted • How authorization and/or supervisory approvals are verified • How a workforce member's level of access to a location is verified Obtain and review documentation of workforce members who were authorized access to ePHI or locations where ePHI might be accessed and organizational charts/lines of authority. Evaluate and determine if access requests were properly authorized in accordance with the entity's related policies and procedures and in accordance with established lines of authority. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and	

			what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Establish a~~ Workforce security -- Workforce Clearance ~~Procedures~~Procedure	§164.308(a)(3) (ii)(B): ~~Workforce Security –~~ Implement ~~policies and~~ procedures to ~~ensure~~determine that ~~all members~~the access of ~~its~~a workforce ~~have appropriate access~~member 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~~ is appropriate.	~~Inquire of management as to whether procedures exist for granting~~Does the entity have policies and procedures in place to determine that a workforce member's access to ePHI is appropriate? Does the entity determine whether a workforce member's access to ePHI is appropriate? Obtain and review documentation related to workforce clearance procedures. Evaluate and determine whether such procedures has been incorporated to determine whether a workforce member's access to ePHI is appropriate. Elements to review may include but are not limited to: • Clearing workforce members prior to authorizing access to ePHI • Revalidation of workforce members' clearance • Frequency of revalidating workforce members' clearance. Obtain and review documentation demonstrating the clearance process prior to granting workforce members access to ePHI. Obtain and review ~~policy and procedures and evaluate the content in relation to~~	Addressable

			~~the relevant specified performance criteria. Obtain and review evidence of~~documentation demonstrating 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~~ (e.g., approved access request forms, electronic approval workflow, etc.). Evaluate and determine if workforce members were granted appropriate access to ePHI based on the clearance process prior to gaining access to ePHI. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	Workforce security -- Establish Termination Procedures	§164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).	~~Inquire of management as to whether there are separate procedures~~Does the entity have policies and procedures in place for terminating access to ePHI when ~~the employment of a workforce member ends, i.e., voluntary termination (retirement, promotion, transfer,~~	Addressable

			~~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~~employment or other arrangements with the workforce member ends? Does the entity terminate access to ePHI when employment or other arrangements with the workforce member ends? Obtain and review policies and procedures for terminating access to ePHI when the employment of, or other arrangement with, a workforce member's employment is terminated or job description changes to require more or less access to ePHI. Evaluate the content in relation to the specified performance criteria. Elements to review may include but are not limited to: • Recovery of access control devices and ~~deactivate computer~~deactivation of information system 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~~, including voluntary termination and involuntary termination • Termination of access by an independent contractor or other business associate, if applicable	

			• Appropriate changes in access levels and/or privileges pursuant to job description changes that necessitate more or less access to ePHI • Time frames to terminate access to ePHI • Exit interviews that include a discussion of privacy and security topics regarding ePHI Obtain and review documentation demonstrating that workforce members' access to ePHI was terminated. Evaluate and determine whether access to ePHI ~~is~~was 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~~ and consistent with related policies and procedures. Obtain and review documentation demonstrating changes in access levels for workforce members with ePHI access. Obtain and review documentation of the job duties of workforce members before and after ePHI access level was changed. Evaluate and determine whether access levels were changed appropriately and in accordance with workforce member job duties. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that	

			the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	Information Access Management	§164.308(a)(4)(i): 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.	Does the entity have policies and procedures in place for authorizing access to ePHI that supports the applicable requirements of the Privacy Rule? Does the entity authorize access to ePHI that supports the applicable requirements of the Privacy Rule? Obtain and review the policies and procedures to determine that they reasonably and appropriately restrict access to only those persons and entities with a need for access. Also obtain entity's policies and procedures related to minimum necessary [45 CFR 164.502(b)] and safeguards [45 CFR 164.514(d)] to determine that the policies and procedures subject to this inquiry support an entity's compliance with the minimum necessary requirement and safeguards requirement that limit unnecessary or inappropriate access to and disclosure of protected health information. Evaluate and determine whether the technical implementation of the access controls used by the entity support the minimum necessary policies and procedures and are consistent with the Privacy Rule safeguard policies.	R

Security	Information Access Management -- Isolating Healthcare Clearinghouse Functions	§164.308(a)(4)(ii)(A): 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.	If the entity is a health care clearinghouse that is part of a larger organization, does the clearinghouse have policies and procedures to protect ePHI from unauthorized access by the larger organization? Does the clearinghouse protect ePHI from unauthorized access by the larger organization? Obtain and review policies and procedures related to protecting ePHI held by a health care clearinghouse from unauthorized access by the larger organization. Evaluate and determine whether reasonable and appropriate administrative, physical, and technical safeguards are in place to protect against unauthorized access by the larger organization.	Required
Security	~~Implement Policies and Procedures for Authorizing~~Information Access Management -- Access Authorization	~~§164.308(a)(4):~~ ~~Information Access Management~~ §164.308(a)(4)(ii)(~~b~~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.	~~Inquire of management as to whether~~Does the entity have policies and procedures ~~are~~ in place to grant access to ePHI~~.~~ for workforce members? Does the entity grant access to ePHI for workforce members? Obtain and review policies and procedures ~~and evaluate~~. Evaluate the content relative to the specified performance 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~~	Addressable

			~~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~~, including whether authority to grant access and the process for granting access has been incorporated. Elements to review may include but are not limited to: • Workforce members or roles required to approve request to create information system accounts • Procedures to create enable, modify, disable, and remove information system accounts • Determination of what the authorization of access is based on Obtain and review documentation associated with granting of access to ePHI (i.e., paper or electronic request). Evaluate and determine if the procedures for granting access to ePHI are in accordance with related policies and procedures. Obtain and review documentation of newly hired workforce members' access to ePHI. Evaluate documentation to determine the granting of access to ePHI, including whether the levels of access they have to systems containing, transmitting, or processing ePHI, are appropriate. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity	

			documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Implement Policies and Procedures for~~ Information Access Management -- Access Establishment and Modification	~~§164.308(a)(4):~~ ~~Information Access Management~~ §164.308(a)(4)(ii)(~~c~~C)~~–~~: Implement policies and procedures that, based upon the covered entity~~'~~'s or the business associate's access authorization policies, establish, document, review, and modify a user~~'~~'s right of access to a workstation, transaction, program, or process.	~~Inquire of management as to whether policies and standards exist to~~Does the entity have policies and procedures in place to authorize access and document, review, and modify a user's right of access to a workstation, transaction, program, or process? Does the entity 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~~the policies and procedures. Evaluate their content relative to the specified performance 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~~	Addressable

			~~they have chosen not to fully implement this specification and their rationale for doing so. Evaluate this documentation if applicable~~ Obtain and review documentation regarding individuals whose access to information systems has been reviewed based on access authorization policies. Evaluate and determine whether individuals' access has been reviewed and recertified in a timely manner by the appropriate personnel. Obtain and review documentation demonstrating individuals whose access to information systems has been modified based on access authorization policies. Evaluate and determine whether modification of access to information systems is acceptable and modification of individuals' access to information systems was completed and approved by appropriate personnel. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	

~~Security~~	~~Isolate Healthcare Clearinghouse Functions~~	~~§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.~~	~~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~~
~~Security~~	~~Evaluate Existing Security Measures Related to Access Controls~~	~~§164.308(a)(4):~~ ~~Information Access Management - 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.~~	~~Inquire of management as to whether formal or informal policies and procedures exist relating to 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.~~	~~Addressable~~
Security	~~Develop~~Security Awareness and ~~Approve a~~ Training	§164.308(a)(5) (i): ~~Security Awareness and Training -~~	~~Inquire of management as to whether security awareness and training programs address the specific required~~	~~Addressable~~Required

	~~Strategy and a Plan~~	Implement a security awareness and training program for all members of its workforce (including management).	~~HIPAA policies. Obtain and review a list of~~Does the entity have policies and procedures in place regarding a 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~~program? Does the entity provide security awareness and training to all new and existing members of its workforce? Obtain and review policies and procedures for security awareness and training program. Elements to review may include but are not limited to: • How workforce members are provided the security awareness and training • Identifies workforce members (including managers, senior executives, and as appropriate, business associates, and contractors) who will be provided with the security and awareness training • How workforce members will be provided with security and awareness training when there is a change in the entity's information systems • How frequently security awareness and training will be provided to all workforce members Obtain and review documentation demonstrating the implementation of a security awareness and training program including related training materials. Evaluate and determine whether the training program	

			is reasonable and appropriate for workforce members to carry out their functions. Obtain and review documentation demonstrating that 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~~ and made available to independent contractors and business associates, if appropriate.	
~~Security~~	~~Develop and Approve a Training Strategy and a Plan~~	~~§164.308(a)(5):~~ ~~Security Awareness and Training - Implement a security awareness and training program for all members of its workforce (including management).~~	~~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~~
Security	~~Protection from~~	§164.308(a)(5)(ii)(~~B~~)~~:~~	~~Inquire of management as to whether~~	Addressable

	~~Malicious Software; Log-in Monitoring;~~ Security Awareness and ~~Password Management~~Training -- Security Reminders	~~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 safeguarding passwords~~A): Periodic security updates.	~~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 specification and their rationale for doing so~~Does the entity have policies and procedures in place regarding a process to provide periodic security reminders and updates? Does the entity appropriately communicate security updates to all members of its workforce and, if appropriate, contractors periodically? Obtain and review documentation demonstrating how periodic security updates are conducted. Elements to review may include but are not limited to: • Frequency of the periodic security updates • Methods of communication used for security updates (i.e. emails, newsletters,	

			posters) Obtain and review documentation demonstrating that periodic security updates are conducted. Evaluate and determine if periodic security updates are accessible and communicated to workforce members. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Develop Appropriate~~Security Awareness ~~and~~, Training ~~Content, Materials~~, and ~~Methods~~Tools -- Protection from Malicious Software	§164.308(a)(5)~~:~~ ~~Security Awareness and Training - Implement a security awareness and training program for all members of its workforce (including management)~~ (ii)(B): Procedures for guarding against, detecting, and reporting malicious software.	~~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~~Does the entity have policies and procedures in place regarding a process to incorporate its procedures to guard against, detect, and report malicious software into its security awareness and training program?	Addressable

			Obtain and review documentation demonstrating that the procedures for guarding against, detecting, and reporting malicious software are incorporated in the security awareness and training program. Elements to review may include but are not limited to: • The malicious software protection mechanism that has been implemented • Information system protection capabilities • Workforce members' roles and responsibilities in malicious software protection procedures • Steps to protect against malicious software • Steps to detect malicious software • Action(s) to be taken in response to malicious software detection Obtain and review documentation demonstrating that procedures are in place to guard against, detect, and report malicious software. Evaluate and determine whether such procedures are in accordance with malicious software protection procedures included in the training material. Obtain and review documentation of the workforce members who should be trained on the procedures to guard against, detect, and report malicious software. Obtain and review documentation of the workforce members who were trained on the procedures to guard against, detect, and report malicious software. Evaluate and determine if appropriate workforce members are being trained on the procedures to guard against, detect, and report malicious software.	

			Has the entity chosen 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~~an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Implement the~~ Security Awareness, Training, and Tools -- Log-in Monitoring	§164.308(a)(5)~~:~~ ~~Security Awareness and Training - Implement a security awareness and training program for all members of its workforce (including management)~~ (ii)(C): Procedures for monitoring log-in attempts and reporting discrepancies.	~~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~~Does the entity have policies and procedures in place to incorporate procedures for monitoring log-in attempts and reporting discrepancies into its security awareness and	Addressable

			training program? Obtain and review procedures (or other vehicle) for monitoring log-in and reporting discrepancies and related training material. Elements to review may include but are not limited to: • Workforce members' roles and responsibilities in monitoring log-in attempts and reporting discrepancies • Identify how log-in monitoring is conducted • How to identify an inappropriate or attempted log-in • Action(s) to be taken in response to an inappropriate or attempted log-in Obtain and review documentation demonstrating that procedures are in place to monitor log-in attempts and report discrepancies. Evaluate and determine whether such procedures are in accordance with the monitoring log-in attempts and reporting discrepancies procedures in the training material. Obtain and review documentation of workforce members and role types of who should be trained on the procedures for monitoring log-in attempts and reporting discrepancies. Obtain and review documentation of the workforce members who were trained on the procedures for monitoring log-in attempts and reporting discrepancies. Evaluate and determine if appropriate workforce members are being trained on the procedures for monitoring log-in attempts and reporting discrepancies.	

			Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Implement~~ Security ~~Reminders~~Awareness, Training, and Tools -- Password Management	§164.308(a)(5)(ii)(~~A~~): ~~Security Awareness and Training - Periodic security updates~~D): Procedures for creating, changing, and safeguarding passwords.	~~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~~Does the entity have policies and procedures in place to incorporate procedures for creating, changing, and safeguarding passwords into its security awareness and training program? Obtain and review password management procedures and training (or other vehicle) for creating, changing, and safeguarding passwords.	Addressable

			Elements to review may include but are not limited to: • Workforce members' roles and responsibilities in the procedures for creating, changing, and safeguarding passwords • Identify how passwords should be created, changed, and safeguarded • Action(s) to be taken in response to a compromised password or other authentication credential Obtain and review documentation demonstrating that procedures for creating, changing, and safeguarding passwords are in place. Evaluate and determine whether such procedures are in accordance with the creating, changing, and safeguarding passwords procedures incorporated into the training material. Obtain and review documentation of workforce members and role types of who should be trained on creating, changing, and safeguarding passwords. Obtain and review documentation of the workforce members who were trained on the procedures for creating, changing, and safeguarding passwords. Evaluate and determine if appropriate workforce members are being trained on the procedures for creating, changing, and safeguarding passwords. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been	

			implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Monitor and Evaluate Training Plan~~Security Incident Procedures	§164.308(a)(~~5):~~ ~~Security Awareness and Training - Implement a security awareness and training program for all members of its workforce (including management)~~ 6)(i): Implement policies and procedures to address security incidents.	~~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~~Does the entity have policies and procedures in place to address security incidents? Obtain and review the policies and procedures related to security incidents Elements to review may include but are not limited to: • Identification of what specific event would be considered a security incident • Identification of workforce members' role and responsibilities regarding security incidents • Management involvement regarding security incidents	~~Addressable~~Required

			• Workforce members or roles to which the incident response policies and procedures are to be disseminated • Coordination of security incidents among business associates • Identifies what steps should be taken in response to a security incident • The frequency to review and update current security incident policies and procedures Obtain and review documentation demonstrating that security incident policies and procedures are implemented. Evaluate and determine whether policies and procedures are appropriate for addressing security incidents and are in accordance with related policies and procedures.	
Security	~~Develop and Implement~~Security Incident Procedures ~~to Respond to --~~ Response and ~~Report Security Incidents~~Reporting	~~§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 or business associate; and document security incidents and their outcomes.	~~Inquire of management as to whether there are formal or informal~~Does the entity have policies and~~/or~~ procedures in place for identifying, responding to, reporting, and mitigating security incidents? Does the entity identify, respond to, report, and mitigate security incidents? Obtain and review policies and procedures related to responding and reporting security incidents. Evaluate and determine if incident response procedures are in place. Elements to review may include but are not limited to: • A methodology for defining security incidents based on levels of criticality • Provisions for reporting and responding to all types of known and suspicious security	Required

			incidents based on criticality levels of such incidents • The roles and responsibilities of workforce members including the entity's security incident response team Obtain and review documentation of responding to, reporting, and mitigating security incidents. ~~Obtain and review the formal or informal policies and procedures~~Evaluate and determine if security incident response, reporting, and mitigation procedures are followed by workforce members; are conducted in ~~place. Obtain and review the formal or informal policies and/or procedures and 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~~a timely manner; and their outcomes are properly documented and communicated to the appropriate workforce members. ~~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.~~	

~~Security~~	~~Develop and Implement Procedures to Respond to and Report Security Incidents~~	~~§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.~~	~~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~~
Security	~~Develop~~ Contingency ~~Planning Policy~~Plan	~~§164.308(a)(7):~~ ~~Contingency Plan~~ §164.308(a)(7)(i) ~~- A contingency plan must be in effect for responding to system emergencies~~: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	~~Inquire of management as to whether~~Does the entity have policies and procedures in place that include 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~~	Required

			~~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~~for responding to an emergency or other occurrences that damages systems that contain ePHI? Does the entity have a contingency plan for responding to an emergency or other occurrences that damages systems that contain ePHI? Obtain and review policies and procedures related to a formal contingency plan. Elements to review may include but are not limited to: • Identification of workforce members' roles and responsibilities in the contingency process • Workforce members or roles to which the contingency policies and procedures are to be disseminated • Management involvement in contingency plans • Coordination of contingency processes among business associates • Identification of what steps should be taken in a contingency plan • The frequency to review and update current contingency policies and procedures	

			• How frequently the contingency plan is tested Obtain and review documentation demonstrating that a contingency plan is implemented. Evaluate and determine that the response to an emergency or other occurrence that damages systems that contain ePHI include appropriate capabilities to recover access to ePHI.	
Security	Contingency Plan – Data Backup Plan ~~and Disaster Recovery 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 restore any loss of data.~~	~~Inquire of management as to~~Does the entity have policies and procedures in place to create and maintain retrievable exact copies of ePHI? Does the entity create and maintain retrievable exact copies of ePHI? Obtain and review policies and procedures related to data back-up plans. Evaluate and determine 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 periodic basis~~data back-up procedures exist that establish strategies for creating and maintaining retrievable exact copies of ePHI should the entity experience an emergency or other occurrence. Elements to review may include but are not limited to:	Required

			• How frequently data backups will be conducted • The type of data that will be backed up • How data will be backed up, including the use of encryption and encryption key management, if applicable • The backup data mechanism/solution • How backup data will be secured • Physical location of backup media • Workforce members' roles and responsibilities in the data backup process • How frequently data backups will be reviewed or assessed for verification of media reliability and data integrity Obtain and review documentation demonstrating how data is backed up. Evaluate and determine whether the data backup process creates exact copies of ePHI. Obtain and review documentation demonstrating data backup and restoration tests. Evaluate and determine if test procedures are in accordance with data backup plans and/or procedures; that test results are properly documented; that test results are reviewed and certified by appropriate management; and, if necessary, that corrective actions have been taken.	
Security	Contingency Plan --Application and Data Criticality Analysis	§164.308(a)(7)(ii)(E): Assess the relative criticality of specific applications and data in support of other contingency plan components.	Does the entity have policies and procedures in place to assess the relative criticality of specific applications and data in support of other contingency plan components? Does the entity assess the relative criticality of specific application and data in support of other contingency plan components?	Addressable

			Obtain and review documentation of critical ePHI applications and their assigned criticality levels. Evaluate and determine if application criticality levels were assessed and categorized based on importance to business needs or patient care, in order to prioritize for data backup, disaster recovery, and emergency operations plans. Obtain and review documentation of the procedures regarding how ePHI applications (data applications that store, maintain or transmit ePHI) are identified. Evaluate and determine whether all critical ePHI applications are identified. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	Contingency Plan – Disaster Recovery Plan	§164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore any loss of data.	Does the entity have policies and procedures in place to restore any lost data? Does the entity restore any lost data? Obtain and review documentation related to a disaster recovery plan. Review and determine if appropriate procedures for restoring any	Required

			loss of data has been incorporated into the disaster recovery plan. Obtain and review procedures for restoring lost data. Evaluate if the procedures include all important sources of data. Elements to review may include but are not limited to: • Workforce members' roles and responsibilities in the process of restoring lost data • Determination of what data will be restored • Step-by-step process of how data will be restored • Identify occurring events (e.g., disruption, compromise, failure) that require data restoration • Timeframe of data restoration • How frequently data restorations will be tested or assessed for verification of media reliability and data integrity Obtain and review documentation of data restore tests and test results. Evaluate and determine if test procedures are in accordance with data restore plans and/or procedures; that test results are properly documented; that test results are reviewed and certified by appropriate management; and, if necessary, corrective actions have been taken.	
Security	~~Develop and Implement an~~ Contingency Plan -- Emergency Mode Operation Plan	§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	~~Inquire of management as to~~Does the entity have policies and procedures in place to enable the continuity of critical business processes for the protection of ePHI while operating in emergency mode?	Required

		electronic protected health information while operating in emergency mode.	Does the entity enable the continuity of critical business processes for the protection of ePHI while operating in emergency mode? Obtain and review procedures related to an emergency mode operation plan. Evaluate and determine whether ~~policy and~~ procedures exist to enable ~~the~~ continuation of critical business processes ~~that protect~~for the protection of the security of ePHI while operating in emergency mode. Obtain and review ~~policy and procedures used to enable~~documentation demonstrating the 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~~. Evaluate and determine if the process is appropriate and/or in accordance with related policies and procedures.	
Security	Contingency Plan -- Testing and Revision Procedure	§164.308(a)(7)(ii)(D): ~~Contingency Plan –~~Implement procedures for periodic testing and revision of contingency plans.	~~Inquire of management as to whether policy~~Does the entity have policies and procedures ~~exist~~ for periodic testing and revisions of its contingency plans? Does the entity periodically test and revise its contingency plans? Obtain and review policies and procedures related to periodic testing and revision of	Addressable

			contingency plans. ~~Obtain and review policy and procedures used for periodic testing and~~ Elements to review may include but are not limited to: • Methods used to test the plan (component, system, or comprehensive) • Workforce members' roles and responsibilities in coordination of the test • How frequently tests will be conducted • How frequently contingency plans will be revised • Notification procedures Obtain and review documentation demonstrating the revision of contingency plans ~~and evaluate the content in relation to the specified criteria. Determine if the policy and procedures~~. Based on related procedures, evaluate and determine if the contingency plans have been approved, reviewed, 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~~ Obtain and review documentation of contingency plan tests and related results. Evaluate and determine if the results of each contingency plan test indicate that tests have been conducted in a timely manner; involved the appropriate workforce members; has been	

			documented; and, if necessary, that corrective actions were taken as result of the contingency plan test. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Identify Preventive Measures~~Business Associate Contracts and Other Arrangements	§164.308(~~a)(7):~~ ~~Contingency Plan §164.308(a)(7)(i) - Preventive Measures must be identified~~b)(1): A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. §164.308(b)(2): A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health	~~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~~Does the entity have policies and procedures in place to obtain satisfactory assurances from its business associates (or business associate subcontractors if the entity is a business associate) and to review the satisfactory assurances to ensure the applicable requirements at § 164.314(a) are included in the business associate contract or other arrangement? Obtain and review documentation identifying all business associates. Obtain and review the business associate agreements and/or contracts. Using sampling methodology,	Required

		information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.	evaluate and determine whether business associate agreements/contracts exist and that security requirements are in place to address the ~~specified criteria.~~ confidentiality, integrity, and availability of ePHI. [This inquiry is for BAs only] Based upon the selection methodologies from the above paragraph, determine whether the business associate contract identifies if it utilizes any subcontractors. If so, review the business associate agreement to examine if (i) Omnibus provisions are required and (ii) all subcontractors who create, receive, maintain, or transmit electronic protected health information on a business associate's behalf maintain business associate agreements equal to or greater than the business associate agreement with the original covered entity. [This inquiry is for BAs only]	
Security	~~Develop Recovery Strategy~~Business Associate Contracts and Other Arrangements -- Written Contract or Other Arrangement	§164.308(~~a)(7):~~ ~~Contingency Plan §164.308(a)(7)(ii)(b) - Establish (and implement as needed) procedures to restore any loss of data~~ b)(3): Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	~~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~~Does the entity have policies and procedures in place to obtain satisfactory assurances from its business associates (or business associate subcontractors if entity is a business associate) and to review the satisfactory assurances to ensure the applicable	Required

			requirements at § 164.314(a) is included in the written contract or other arrangement? Obtain and review documentation of all business associates. Obtain and review the written agreements or other arrangements (i.e., a Memorandum of Understanding if the covered entity and business associate are government agencies). Using sampling methodology, evaluate and determine whether a written contract or other arrangement exist and that security requirements are in place to address the confidentiality, integrity, and availability of ePHI. (NOTE: Business associate contracts should have been updated in 2013) [This inquiry is for BAs only] Based upon the selection methodologies from the above paragraph, evaluate and determine whether the written contract or other arrangement identifies if there are any subcontractors. If so, review the written contract or other arrangement to examine if (i) Omnibus provisions are required and (ii) all subcontractors who create, receive, maintain, or transmit electronic protected health information on a business associate's behalf maintain business associate agreements equal or greater than the business associate agreement with the original covered entity. [This inquiry is for BAs only]	
Security	~~Data Backup Plan and Disaster Recovery Plan~~Facility Access	§~~164.308(a)(7):~~ ~~Contingency Plan §164.308(a)(7)(ii)(a) - Establish and~~	~~Inquire of management as to whether written~~Does the entity have policies and procedures ~~exist~~in place regarding access to ~~create and maintain exact copies of~~	Required

	Controls	implement164.310(a)(1): Implement policies and procedures to create and maintain retrievable exact copies of limit physical access to [an entity's] electronic protected health information. Contingency Plan §164.308(a)(7)(ii)(b) - Establish (and implement as needed) procedures to restore any loss of datainformation systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	ePHI. Obtain and review procedures and evaluateand use of facilities and equipment that house ePHI? Does the entity limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed? Obtain and review policies and procedures regarding facility access control. Evaluate the content in relation to the relevant specified criteria used to create and maintain exact copies of ePHI. Determine if the procedure has been approved and updated on a periodic basisperformance criteria regarding physical access to electronic information systems and use of facilities and equipment that house ePHI. Evaluate and determine if policies and procedures identify the countermeasures implemented to control physical access and to detect, deter, and/or prevent unauthorized access and unlimited access to electronic information systems and facilities where systems are housed. Elements to review may include but are not limited to: • Workforce members' roles and responsibilities in facility access control procedures • Management involvement in the facility's access controls procedures • The process of how authorization credentials for facility access are issued	

			• The process of removing workforce members' authorization credentials for physical access when such access it is no longer required • Identification of how visitors' access is monitored • Methods for controlling and managing physical access devices • Facilities and areas that have physical access control implemented to safeguard ePHI Obtain and review documentation of workforce members with authorized physical access to electronic information systems and the facility or facilities in which they are housed. Evaluate and determine if authorized workforce members are listed in areas where electronic information system resides; listed authorized members have been approved by appropriate management; list of authorized workforce members are reviewed on a continuous basis; and removed when access is no longer required. Obtain and review documentation of procedures for granting individuals access to entity facility or facilities where electronic information systems are housed. Evaluate and determine if physical access authorization is enforced at entry/exit points of the facility; individual access authorization is verified before granted access to facility; and physical access audit logs of entry/exit points are maintained and reviewed on continuous basis. Obtain and review documentation of visitor physical access to electronic information systems and the facility or facilities where it is housed. Evaluate and determine if visitors	

			are supervised in locations where electronic information resides and if activities are documented and monitored.	
~~Security~~	~~Determine Whether Internal or External Evaluation Is Most Appropriate~~	~~§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.~~	~~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~~
~~Security~~	~~Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule~~	~~§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.~~	~~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~~

~~Security~~	~~Conduct Evaluation~~	~~§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.~~	~~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~~
~~Security~~	~~Document Results~~	~~§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.~~	~~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 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.~~	~~Required~~

~~Security~~	~~Repeat Evaluations Periodically~~	~~§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.~~	~~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 secu rity 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~~
~~Security~~	~~Written Contract or Other Arrangement~~	~~§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.~~	~~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~~

~~Security~~	~~Implement An Arrangement Other than a Business Associate Contract if Reasonable and Appropriate~~	~~§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 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.~~	~~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~~
~~Security~~	~~Conduct an Analysis of Existing Physical Security Vulnerabilities~~	~~§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.~~	~~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~~	~~Addressable~~

			~~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.~~	
~~Security~~	~~Develop a Facility Security Plan~~	~~§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.~~	~~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~~

~~Security~~	~~Establish Contingency Operations Procedures~~	~~§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.~~	~~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, 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.~~	~~Addressable~~
Security	~~Establish~~ Facility Access Controls -- Contingency Operations ~~Procedures~~	§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.	~~Inquire of management to determine if formal or informal documentation exists~~Does the entity have policies and procedures in place 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~~? Does the entity allow facility access for the restoration of lost data under the Disaster Recover Plan and Emergency Mode Operation Plan in the event of an emergency? Obtain and review contingency operations procedures. Evaluate the content in relation to	Addressable

			the specified performance 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~~ in the event of all types of potential disasters. Elements to review may include but are not limited to: • Identification of who will need access to ePHI in the event of a disaster • Backup up plan for access to the facility and/or ePHI • Workforce member roles and responsibilities from implementing the contingency plan for accessing ePHI in each department, unit, etc. • Procedures for accessing restored data at the alternate processing, storage, and work site • Procedures for the testing contingency operations Obtain and review documentation demonstrating contingency operation procedures currently implemented. Evaluate and determine if processes are in accordance with related policies and procedures. Obtain and review documentation	

			demonstrating that contingency operation procedures are tested. Evaluate and determine if testing is conducted on a periodic basis and testing results are documented, including a plan of corrective actions, if necessary. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	Facility Access Controls -- Facility Security Plan	§164.310(a)(2)(ii): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Does the entity have policies and procedures in place to safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft? Does the entity safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft? Obtain and review policies and procedures related to the facility security plan. Evaluate the content in relation to the specified performance criteria for safeguarding the facility and equipment therein from unauthorized physical access, tampering, and theft. Elements to review may include but are not limited to:	Addressable

			• Identification of the physical security measures in place to provide physical security protection for facilities and equipment • Workforce members' roles and responsibilities regarding the facility security plan • Inventory of the entity's facilities that house equipment that create, maintain, receive, and transmit ePHI Obtain and review documentation demonstrating that facility security plan procedures are implemented to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Evaluate and determine if implementation of the facility security plan is being followed appropriately and is in accordance with related policies and procedures. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	Facility Access Controls -- Access Control and Validation Procedures	§164.310(a)(2)(iii): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control,	Does the entity have policies and procedures in place for controlling a person's access to facilities based on their role or function including visitor control and control of access	Addressable

		and control of access to software programs for testing and revision	to software programs for testing and revision? Does the entity control a person's access to facilities based on their role or function including visitor control and control of access to software programs for testing and revision? Obtain and review procedures related to access control and validation. Evaluate the content in relation to the specified performance criteria for controlling a person's facility access including workforce members, contractors, visitors and probationary employees. Elements to review may include but are not limited to: • Methods for controlling and validating an employee's access to the facility • Workforce members' roles and responsibilities in the access control and validation process • Frequency of reviewing lists of individuals with physical access to sensitive facilities • Methods to control visitor's physical access to facilities Obtain and review documentation demonstrating the control of visitor's physical access to facilities. Evaluate and determine if physical controls identify visitors attempting to access facility, prevent unauthorized visitors, and grant access to authorized visitors. Obtain and review documentation demonstrating control of access to software program for modification and revision. Evaluate and determine if authorized	

			individuals, roles, or job functions are identified and validated before gaining access to software program and is in accordance with applicable procedures. Obtain and review documentation demonstrating facility and software access control and validation procedures are implemented. Evaluate and determine if safeguards implemented overall controls access to facility physical environment, by validating individuals roles or function before granting physical access to facility or software programs; deter and prevent unauthorized access to the facility or software in accordance with applicable policies and procedures. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	Facility Access Controls -- Maintain Maintenance Records	§164.310(a)(2)(~~iV):~~ ~~Facility access controls -~~ iv): Implement policies and procedures to document repairs and modifications to the	~~Inquire of management as to whether~~Does the entity have policies and procedures ~~exist~~in place to document repairs and modifications to the physical components of a facility ~~that~~which are related to security~~.~~	Addressable

		physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	? Does the entity document repairs and modifications to the physical components of a facility which are related to security? Obtain and review ~~policy~~such policies and procedures ~~and evaluate~~related to maintaining maintenance records. Evaluate the content in relation to the specified performance 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~~ Elements to review but are not limited to: • Workforce members' roles and responsibilities in repairs and modification to the physical components • Record keeping process of repairs and modification to the physical components • Specification of when repairs or modification of physical security components are required • Authorization process of repairs or modification of physical security components Obtain and review documentation demonstrating records of repairs and modifications to physical security	

			components. Evaluate and determine if records of repairs and modifications are being tracked and reviewed on periodic basis by authorized personnel. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Identify~~ Workstation ~~Types and Functions or Uses~~Use	§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.	~~Inquire of management as to whether a process exists for identifying workstations by type and location. Obtain and review formal or informal~~Does the entity have policies and procedures in place that specifies the proper functions to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI? Does the entity specify the proper functions to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI? Obtain and review such policies and procedures ~~and evaluate~~related to workstation use. Evaluate the content in	Required

			relation to the specified ~~criteria for identifying~~performance criteria for the proper functions to be performed by electronic computing devices. Elements to review may include but are not limited to: • Process to identify workstations by type and location~~. Determine if each workstations~~ • Specify the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI (e.g. to prevent or preclude unauthorized access to an unattended workstation, limit the ability of unauthorized persons to view sensitive information as needed) • Procedures related to the proper use and performance of workstations • Workforce members roles and responsibilities in the workstation use process Obtain and review an inventory of the locations and types of workstations. Evaluate and determine if an inventory exists of workstation; when the inventory was last updated; and whether there is a documented process for updating the inventory. If available, review the inventory to see if it includes the types of ePHI data elements contained on the systems included in the inventory. Obtain documentation demonstrating workstation classification. Evaluate and determine if each workstation is classified based on the specific workstation's capabilities, connection, and allowable activities.	

			Obtain and review documentation demonstrating workstation use policies and procedures implemented. Evaluate if such implementation is in accordance with related policies and procedures.	
~~Security~~	~~Identify Expected Performance of Each Type of Workstation~~	~~§164.310(b):~~ ~~Workstation Use - Covered entities must 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~~
~~Security~~	~~Analyze Physical Surroundings for Physical Attributes~~	~~§164.310(b):~~ ~~Workstation Use - Covered entities should 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~~

Security	~~Identify All Methods of Physical Access to Workstations~~Workstation Security	§164.310(c): ~~Workstation Security §164.310(b) - Covered entities should implement~~Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	~~Inquire of management as to~~Does the entity have policies and procedures that document 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~~? Does the entity workstations that access electronic protected health information restricted to authorized users? Obtain and review policies and procedures related to workstation security. Evaluate the content in relation to the specified criteria for security measures and guidance on how to implement and 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~~ and how physical access to workstations that access ePHI is	Required

			restricted to appropriate personnel. Obtain and review documentation demonstrating workstation security policies and procedures being implemented. Evaluate and determine if implementation is appropriate and is in accordance with related policies and procedures.	
Security	~~Identify~~Device and ~~Implement Physical Safeguards for Workstations~~Media Controls	§164.310(~~c):~~ ~~Workstation Security §164.310(b) - Covered entities should implement physical safeguards for all workstations that access~~d)(1): Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, ~~to restrict access to authorized users~~into and out of a facility, and the movement of these items within the facility.	~~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~~Does the entity have policies and procedures in place that govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility? Does the entity govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within facility? Obtain and review the policies and procedures related to device and media	Required

			controls. Evaluate the content in relation to the specified performance criteria for the proper handling of electronic media that contain ePHI. Elements to review may include but are not limited to: • How are the types of hardware and electronic media that must be tracked (both entity owned and personally owned) are identified • The process of tracking all types of hardware and electronic media that contain ePHI • Workforce members' roles and responsibilities in the device and media control process • Authorization process for the receipt and removal of hardware and electronic media that store ePHI • How the release of hardware, software, and ePHI data out of entity control is ~~communicated and how the user acknowledges the information contained within. Observe the premises to determine if doors have locks, cameras are in place, security guards are in place, etc.~~ managed and documented Obtain and review documentation demonstrating the movement of hardware and electronic media containing ePHI into, out of and within the facility. Evaluate and determine if movement of hardware and electronic media is being properly tracked, documented, and approved by appropriate personnel.	

			Obtain documentation demonstrating the type of security controls implemented for the facility in, out, and within movements of workforce members' assigned hardware and electronic media that contain ePHI. Evaluate and determine if security controls are appropriate, properly implemented, and minimize possible vulnerabilities.	
Security	~~Implement Methods for Final~~ Device and Media Controls -- Disposal ~~of ePHI~~	~~§164.310(d)(1):~~ ~~Device and Media Controls -~~ §164.310(d)(2)(i) : Implement policies and procedures to address the final disposition of ~~ePHI~~electronic protected health information and/or the hardware or electronic media on which it is stored.	~~Inquire of management as to how the disposal of hardware, software, and ePHI data is managed.~~ Does the entity have policies and procedures that address the disposal ePHI data, hardware or electronic media on which it is stored? Does the entity address the disposal ePHI data, hardware or electronic media on which it is stored? Obtain and review ~~formal~~ policies and procedures ~~and evaluate~~related to disposal of any electronic media that stores ePHI. Evaluate the content ~~relative~~in relation to the specified performance criteria ~~regarding~~for 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~~. Elements to review may include but are not limited to: • How the disposal of ePHI and or the	Required

			hardware or electronic media that stores ePHI is managed and documented • Identification of how the sanitization process of information system media is managed and documented • Workforce members' roles and responsibilities in the device and media disposal process • Identification of how the disposition of previous stored ePHI and/or the hardware or electronic media is verified • Identify the types of devices and media that store ePHI Obtain and review documentation demonstrating how the disposal of hardware, software, and ePHI data is completed, managed, and documented. Evaluate and determine if process is being followed appropriately and is in accordance with related policies and procedures. Obtain and review documentation demonstrating how the sanitization of electronic media is completed, managed, and documented. Evaluate and determine if process is being followed appropriately and is in accordance with related policies and procedures.	

~~Security~~	~~Maintain Accountability for Hardware and Electronic Media~~	~~§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.~~	~~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~~

~~Security~~	~~Develop Data Backup and Storage Procedures~~	~~§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.~~	~~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 procedures and evaluate the content relative to the specified criteria to determine how often restoration tests~~	~~Addressable~~

		~~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.~~	

~~Security~~	~~Develop Data Backup and Storage Procedures~~	~~§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.~~	~~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~~	~~Addressable~~

			~~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.~~	
Security	~~Develop and Implement Procedures for Reuse of Electronic~~Device and	~~§164.310(d)(1):~~ ~~Device and Media Controls -~~ §164.310(d)(2)(ii) : Implement procedures for removal of ~~ePHI~~electronic	~~Inquire of management as to the processes~~Does the entity have policies and procedures established to remove ePHI before reusing electronic media and who is responsible for the overseeing those processes~~.~~?	Required

	Media Controls -- Media Re-use	protected health information 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~~ re-use. ~~Ensure that ePHI is removed from reusable media before they are used to record new information.~~	Does the entity remove ePHI before reusing electronic media and who is responsible for the overseeing those processes? Obtain and review ~~policies and~~ procedures ~~and evaluate~~related to media re-usage. Evaluate the content in relation to the specified performance criteria for removing ePHI from electronic media before they are issued for reuse. Elements to review may include but are not limited to: • Workforce members' roles and responsibilities in the media re-use process • How the removal of ePHI from electronic media is verified • How ePHI will be removed from electronic media before external and internal re-use Obtain documentation demonstrating media re-use procedures being implemented and how ePHI has been removed from electronic media. Evaluate and determine if the process used for the reuse of electronic media is appropriate; that ePHI is properly removed from electronic media prior to reuse; that ePHI that is removed is unusable, inaccessible, and indecipherable; and that removal of ePHI from electronic media has been verified prior to reuse of electronic media.	
Security	~~Encryption~~Device and ~~Decryption~~Media Controls --	§~~164.312(a)(1):~~ ~~Access Control - §164.312(a)(2)(iv)~~	~~Inquire of management as to whether an encryption mechanism is in place to protect ePHI.~~ Does the entity have policies and procedures to record the movements of	Addressable

	Accountability	~~Implement a mechanism to encrypt and decrypt~~164.310(d)(2)(iii): Maintain a record of the movements of hardware and electronic ~~protected health information~~media and any person responsible therefore.	hardware and electronic media and any person responsible therefore? Does the entity record the movements of hardware and electronic media and any person responsible therefore? Obtain and review ~~formal or informal~~ policies and procedures ~~and evaluate~~related to device and media accountability. 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~~performance criteria regarding tracking the location of electronic media and hardware (including entity-owned and personally-owned electronic/mobile devices and media containing, or with access to, ePHI) and maintaining records of movements of, and individual(s) responsible for, hardware and electronic media that has access or contains ePHI. Elements to review may 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~~ • Workforce members' roles and responsibilities in the device and media accountability process • How records of movements of electronic media and hardware are maintained • The processing of reviewing and certifying movements of hardware and electronic media	

			records • Identify the types of hardware and electronic media that will be tracked in the device and media accountability process Obtain and review documentation demonstrating a record of movements of hardware and electronic media and person responsible therefore. Evaluate and determine if media and hardware (including entity-owned and personally owned electronic/mobile devices and media) are tracked, recorded, and certified by appropriate personnel. Has the 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~~an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Analyze Workloads~~Device and ~~Operations to Identify the Access~~	§~~164.312(a)(1):~~ ~~Access Control - Implement technical policies and procedures for~~	~~Inquire of management as to how the workloads and operations are analyzed to determine the access needs of all users within the entity.~~ Does the entity	~~N/A~~Addressable

	~~Needs of All Users~~Media Controls -- Data Backup and Storage Procedures	~~electronic information systems that maintain~~164.310(d)(2)(iv): Create a retrievable, exact copy of 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)~~ , when needed, before movement of equipment.	have policies and procedures in place to create a retrievable, exact copy of ePHI when needed, before movement of equipment? Does the entity create retrievable, exact copy of ePHI when needed, before movement of equipment? Obtain and review policies and procedures related to data backup and storage procedures. Evaluate the content relative to the specified performance criteria to determine whether policies and procedures cover creating a retrievable exact copy of electronic protected health information, when needed, before movement of equipment. Elements to review may include but are not limited to: • Identify when ePHI data backups will be conducted • The type of data that will be backed up • How data will be backed up, including the use of encryption and encryption key management, if applicable • Backup data mechanism/solution • How backup data is secured • Identification of how and where backup ePHI data is physically stored and secured • Workforce members' roles and responsibilities in the data backup and storage process • How frequently data backups are reviewed or assessed for verification of media reliability and data integrity 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~~demonstrating how ePHI data is backed up for equipment being moved to another location. Evaluate and determine if ePHI data backup process is appropriate and is in accordance with the entity's data backup plan and/or procedures. Obtain and review documentation demonstrating how ePHI data backups for moved equipment are stored. Evaluate and determine if the backup data is stored in a location with minimum vulnerabilities and appropriate safeguards and that the confidentiality, integrity, and availability of the ePHI data is protected from security threats. Obtain and review documentation demonstrating the restoration of ePHI data backups for moved equipment. Evaluate and determine if the procedure is in accordance with backup plans and/or procedures; if failures of data backups and restorations are properly documented; and if necessary, what corrective actions have been taken. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is	

			equivalent to the protections afforded by the implementation specification.	
~~Security~~	~~Identify Technical Access Control Capabilities~~	~~§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).~~	~~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~~
~~Security~~	~~Ensure that All System Users Have Been Assigned a Unique Identifier~~	~~§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.~~	~~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 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.~~	~~Required~~
Security	~~Develop~~ Access	§164.312(a)(1):	~~Inquire of management to determine if~~	~~N/A~~Required

	Control ~~Policy~~	~~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).	~~there is an access control policy in place. Obtain and review policies and/or procedures~~Has the entity implemented technical policies and procedure for the electronic information systems that maintain ePHI to allow access only to authorized users? Does the entity only allow access to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) to electronic information systems that maintain electronic protected health information? Obtain and review policies and procedures related to access control. Evaluate the content relative to the specified performance criteria to determine if ePHI is only accessible to authorized persons or software programs. Elements to review may include but are not limited to: • Identification of the capabilities of electronic information system access controls (i.e., read-only, modify, full access) • Identification of the type of access controls implemented for the electronic information systems • Identification of how system and generic IDs/accounts are implemented, managed and controlled by technical access controls • Workforce members' roles and responsibilities regarding the capabilities to add, modify, or delete user access • The frequency of review and verification of user access to electronic information systems that maintain ePHI	

			• The frequency of review and verification of software program access to electronic information systems that maintain ePHI • How is removed upon termination or modified upon change of position Obtain and review documentation demonstrating the implementation of access controls for electronic information systems that maintain ePHI. Evaluate and determine if the electronic information systems have the capacity to enable access controls; if access controls can be enabled, are the enabled access controls configured in accordance with the access control policies and procedures; and how are the electronic information systems' technical access capabilities defined (i.e., read-only, modify, full-access). Obtain and review documentation demonstrating a list of new workforce members from the electronic information system who was granted access to ePHI. Obtain and review documentation demonstrating the access levels granted to new workforce members. Evaluate and determine whether workforce members' access was approved; review the new workforce members' technical access granted and compare it to approved user access to determine that technical access is approved and granted in accordance with the access authorization requirements. Obtain and review documentation of a list of users with privileged access. Evaluate and determine whether the privileged access is appropriate based on the access control policies.	

			Obtain and review a list of default, generic/shared, and service accounts from the electronic information systems with access to ePHI. Obtain and review documentation demonstrating the access levels granted to default, generic/shared, and service accounts. Evaluate and determine if the default, generic/shared, and service accounts are in use and that access has been approved and granted in accordance with the access authorization requirements. Obtain and review documentation demonstrating that periodic reviews of procedures related to access controls have been conducted. Evaluate and determine whether reviews have been performed of user access levels 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~~performance criteria. Obtain and review documentation demonstrating a list of terminations and job transfers. Obtain documentation demonstrating the removal or modification of user access levels. Evaluate and determine whether user access level removal or modification was approved and performed in accordance with the related policies and procedures.	

~~Security~~	~~Implement Access Control Procedures Using Selected Hardware and Software~~	~~§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).~~	~~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~~
~~Security~~	~~Implement Access Control Procedures Using Selected Hardware and Software~~	~~§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).~~	~~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~~
~~Security~~	~~Implement Access Control Procedures Using Selected Hardware and Software~~	~~§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~~	~~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~~	~~N/A~~

		~~as specified in § 164.308(a)(4).~~	~~appropriate based on policy in place.~~	
Security	~~Review and Update User~~ Access Control -- Unique User Identification	§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)~~ 2)(i): Assign a unique name and/or number for identifying and tracking user identity.	~~Inquire of management as to whether user access to systems and applications is reviewed on a periodic basis.~~ Does the entity have polices and procedures regarding the assignment of unique user IDs to track user identity? Does the entity assign unique user IDs to track user identity? Obtain and review policies and~~/or~~ procedures ~~to determine whether formal procedures are in place over the review~~regarding the assignment of unique user ~~access that address the recommended performance criteria, such as enforcing~~IDs. Evaluate the content of the policies and procedures ~~as a matter of ongoing operations; determining whether changes are needed based on periodic reviews; and establishing and updating access.~~ in relation to the specified performance criteria to determine how user IDs are to be established and assigned. Obtain and review documentation ~~to determine whether reviews have been~~	~~N/A~~Required

			~~performed over user access and evaluate the content in relation to the specified criteria for reviews~~demonstrating the assignment, creation, and use of unique user IDs in electronic information systems for user. Evaluate and determine if users are assigned a unique ID in accordance with the entity's policies and procedures for attributing new user IDs.	
Security	~~Establish an~~ Access Control --- Emergency Access Procedure	§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.~~	~~Inquire of management as to whether an emergency access procedure is in place for obtaining necessary~~Does the entity have polices and procedures in place to provide access to ePHI during an emergency~~.~~ ? Does the entity provide access to ePHI during an emergency? Obtain and review ~~policies and/or~~ procedures ~~and evaluate~~related to emergency access. 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. Elements to review may include but are not limited to: • Procedures in place to provide necessary access to ePHI during an emergency • How access to initiate emergency access to ePHI is limited to appropriate personnel • How access to ePHI is normalized once an emergency situation has passed • Workforce members roles and	Required

			responsibilities in the emergency access procedures Obtain and review documentation demonstrating a list of workforce members with authority to initiate the emergency access procedures. Evaluate and determine if list of workforce members correlates with workforce members listed in the emergency access procedures. Obtain and review documentation demonstrating technical systems limiting emergency access initiation. Evaluate and determine whether technical systems have the capability to limit emergency access initiation to authorized workforce members only.	
~~Security~~	~~Establish an Emergency Access Procedure~~	~~§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.~~	~~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~~
Security	Access Control -- Automatic Logoff	§164.312(a)(2)(iii): ~~Access Control --~~Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	~~Inquire of management as to whether automatic logoff occurs~~Does the entity have policies and procedures in place to automatically terminates an electronic session after a predetermined time of inactivity~~.~~ ? Does the entity automatically terminates an electronic session after a predetermined time	Addressable

			of inactivity? Obtain and review policies and~~/or~~ procedures ~~and evaluate~~regarding automatic logoff. Evaluate the content in relation to the specified criteria to determine whether ~~they specify that automatic logoff occurs~~it specifies that an electronic session is terminated after a predetermined time of inactivity. Obtain and review ~~screenshots to determine that~~documentation (e.g., screenshots, system settings, etc.) demonstrating the implementation of automatic logoff. Evaluate and determine if automatic logoff settings are implemented ~~and conform to the established~~in accordance with related policies and~~/or~~ procedures.~~ Obtain and review screenshots of the encryption configuration over ePHI~~ Has the entity chosen to implement an alternative measure? If yes, obtain and review documentation of why it was determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate the documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	

Security	~~Terminate~~ Access ~~if it is No Longer Required~~Control -- Encryption and Decryption	§164.312(a)(~~1~~2)(iv): ~~Access Control - Implement technical policies and procedures for electronic information systems that maintain~~Implement a mechanism to encrypt and decrypt 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)~~.	~~Inquire of management as to how user access is removed upon termination or change of position on a timely basis. Obtain and review policies and/or~~Does the entity have policies and procedures in place to encrypt and decrypt ePHI including processes regarding the use and management of the confidential process or key used to encrypt and decrypt ePHI? Does the entity encrypt and decrypt ePHI including processes regarding the use and management of the confidential process or key used to encrypt and decrypt ePHI? Obtain and review the policies and procedures ~~and evaluate~~regarding the encryption and decryption of ePHI. Evaluate the content ~~in relation~~relative 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~~	~~N/A~~Addressable

			~~on a timely basis~~that the implementation and use of encryption appropriately protects ePHI. Elements to review may include but are not limited to: • Type(s) and documentation of encryption technology used for devices and media that contain or have access to ePHI • How the confidential processes or keys used for encryption and decryption are managed and protected • How access to modify or create keys is restricted to appropriate personnel Obtain and review documentation demonstrating ePHI being encrypted and decrypted. Evaluate and determine if ePHI is encrypted and decrypted in accordance with related policies and procedures. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Determine the Activities that Will be Tracked or Audited~~Audit	§164.312(b): ~~Audit controls-~~ Implement hardware, software, and/or procedural mechanisms	~~Inquire of management as to whether audit controls have been implemented over~~Does the entity have policies and procedures in place to implement hardware,	Required

	Controls	that record and examine activity in information systems that contain or use electronic protected health information.	software and/or procedural mechanisms to record and examine activity in information systems that contain or use ePHI. ~~-~~? Does the entity have hardware, software and/or procedural mechanism to record and examine activity in information systems that contain or use ePHI? Obtain and review documentation relative to ~~the specified criteria to determine~~audit controls. Evaluate whether risk-based audit controls have been implemented over all electronic information systems that contain or use ePHI. Elements to review may include but are not limited to: • Identification of the risk-based audit controls over all information systems that contain or use ePHI • How are systems and applications evaluated to determine if auditing controls should be implemented • Identification of what applications and systems will be audited • Procedures on how systems will be audited Obtain and review documentation demonstrating the implementation of hardware, software and/or procedural mechanisms to record and examine activity. Evaluate and determine whether information systems that contain or use ePHI activities are being recorded and examined; activities being recorded and examined appropriately and in accordance with related policies and procedures.	

~~Security~~	~~Select the Tools that Will be Deployed for Auditing and System Activity Reviews~~	~~§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.~~	~~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~~
~~Security~~	~~Develop and Deploy the Information System Activity Review/Audit Policy~~	~~§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.~~	~~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~~
~~Security~~	~~Develop Appropriate Standard Operating Procedures~~	~~§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.~~	~~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~~

Security	~~Identify All Users Who Have Been Authorized to Access ePHI~~Integrity	§164.312(c)(1): ~~Integrity:~~ Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	~~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~~Does the entity have policies and procedures in place to protect ePHI from improper alteration or destruction? Does the entity protect ePHI form improper alteration or destruction? Obtain and review policies and procedures regarding the implementation of integrity controls to protect ePHI. Evaluate if the implemented integrity controls appropriately protect the entity's ePHI from improper alteration or destruction. Elements to review may include but are not limited to: • What processes are in place to protect ePHI from improper alteration or destruction • How processes protect ePHI from improper alteration or destruction • How processes detect improper alteration or destruction of ePHI • What actions are taken if improper alteration or destruction of ePHI is detected Obtain and review documentation demonstrating processes in place to protect ePHI from improper alteration or destruction. Evaluate and determine whether ~~users who should have access to ePHI have been identified and evaluate this documentation against specified criteria.~~ implementation of process in in	~~N/A~~Required

			accordance with related policies and procedures. Obtain and review documentation demonstrating processes protecting ePHI from improper alteration or destruction. Evaluate and determine whether ePHI is properly protected from alteration or destruction; processes in place to protect ePHI correlates with safeguards identify in integrity control policies and procedures.	
~~Security~~	~~Implement Procedures to Address These Requirements~~	~~§164.312(c)(1):~~ ~~Integrity - Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.~~	~~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~~
Security	~~Implement a~~ Integrity -- Mechanism to Authenticate ePHI	§164.312(c)(2)~~–~~: Implement electronic mechanisms to corroborate that ~~ePHI~~electronic protected health information has not been altered or destroyed in an unauthorized manner.	~~Inquire~~Does the entity have policies and procedures in place regarding the implementation of ~~management as to whether electronic mechanisms are in place to authenticate ePHI. Obtain and review documentation and evaluate~~electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?	Addressable

			Does the entity have electronic mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner? Obtain and review policies and procedures for authenticating ePHI. 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~~ Elements to review include but are not limited to: • How to detect if ePHI has not been altered or destroyed • How to detect if ePHI has been altered or destroyed in an unauthorized manner. Obtain and review documentation demonstrating that electronic mechanisms are implemented to authenticate ePHI. Evaluate the implemented mechanisms to determine that the implemented mechanisms would appropriately corroborate that ePHI has not been altered or destroyed in an unauthorized manner. Has the entity chosen 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~~an alternative measure?	

			If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	~~Determine~~Person or Entity Authentication ~~Applicability to Current Systems/Applications~~	~~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~~§164.312(d): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	~~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~~Does the entity have policies and procedures in place to verify that a person or entity seeking access to ePHI is the one claimed? Does the entity verify that a person or entity seeking access to ePHI is the one claimed? Obtain and review policies and procedures regarding person or entity authentication. Evaluate if systems and applications requiring authentication have been identified and whether authentication ~~methods~~procedures have been ~~researched and identified~~implemented for the ~~entity's~~ systems and applications that require authentication. Elements to review may include but are not limited to: • The authentication procedures for all systems and applications that access ePHI. • Procedures to evaluate information systems	Required

			and application authentication methods. • The authentication process for verifying identity of a real person or an automated process or entity. Obtain and review documentation demonstrating the implementation of authentication procedures for persons or entities seeking access to ePHI. Evaluate and determine whether the implemented authentication procedures are sufficient to verify that the persons or entity seeking access to ePHI is the one claimed.	
~~Security~~	~~Evaluate Authentication Methods Available~~	~~§164.312(d):~~ ~~Person or Entity Authentication - Weigh the relative advantages and disadvantages of commonly used authentication 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.~~	~~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. 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.~~	~~Required~~

~~Security~~	~~Select and Implement Authentication Option~~	~~§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.~~	~~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~~
~~Security~~	~~Select and Implement Authentication Option~~	~~§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.~~	~~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~~
Security	~~Develop and Implement~~ Transmission ~~Security Policy and Procedures~~	§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	~~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~~Does the entity have policies and procedures in place to	~~N/A~~Required

		communications network.	implement technical security controls to guard against unauthorized access to ePHI transmitted over electronic communications networks? Does the entity have security controls to guard against unauthorized access to ePHI transmitted over electronic communications networks? Obtain and review policies and procedures related to transmission security controls. Evaluate content relative to the specified criteria to determine that the technical security controls implemented guards against unauthorized access to ePHI transmitted over electronic communication networks. Elements to review may include but are not limited to: • Identify the various methods, devices, and networks used to electronically transmit ePHI • The procedures to evaluate and select appropriate technical controls to secure ePHI transmitted across all of its devices and networks • Identify the technical security controls implemented to guard against unauthorized access to ePHI transmitted over electronic communication networks Obtain and review documentation demonstrating the implementation of technical security measures to protect electronic transmissions of ePHI. Evaluate the content in relation to the specified criteria to determine that the implemented technical security measures are sufficient to guard against unauthorized access to the	

			electronically transmitted ePHI.	
Security	Transmission Security -- Integrity Controls	§164.312(e)(2)(i): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Does the entity have policies and procedures in place to implement security measures to ensure that electronically transmitted ePHI cannot be improperly modified without detection until disposed of. Obtain and review policies and procedures related to transmission security measures. Evaluate content relative to the specified criteria to determine that the security measures are implemented to ensure that electronically transmitted ePHI cannot be improperly modified without detection. Elements to review may include but are not limited to: • The security measures in place to ensure that electronically transmitted ePHI has not been improperly modified without detection • How to detect if transmitted ePHI has been improperly modified Obtain and review documentation demonstrating the implementation of security measures to protect electronic transmissions of ePHI. Evaluate the content to determine if the implemented security measures ensure that electronically transmitted PHI cannot be improperly modified without detection. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and	Addressable

			what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	Transmission Security --Encryption	§164.312(e)(2)(ii): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Does the entity have policies and procedures in place to implement an encryption mechanism to encrypt ePHI whenever deemed appropriate? Does the entity have encryption mechanism to encrypt ePHI whenever deemed? Obtain and review policies and procedures regarding the encryption of electronically transmitted ePHI. Evaluate the content relative to the specified criteria to determine that the implementation and use of encryption appropriately secures electronically transmitted ePHI. Elements to review may include but are not limited to: • Type(s) and documentation of encryption technology used to secure electronically transmitted ePHI • How the confidential processes or keys used for encryption are managed and protected • How access to modify or create keys is restricted to appropriate personnel • Identify when it is appropriate to encrypt ePHI Obtain and review documentation demonstrating the encrypted mechanism is implemented to encrypt ePHI. Evaluate and	Addressable

			determine whether encrypted mechanism has the capability to encrypt ePHI when it is deemed as appropriate. Obtain and review documentation demonstrating that electronically transmitted ePHI is encrypted. Evaluate and determine if ePHI encrypted is appropriate and in accordance with related policies and procedures. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	
Security	Policies and Procedures	§164.316(a): Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are	Does the entity have policies and procedures in place to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specification or other requirements of the Security Rule? Obtain and review documentation of the policies and procedures regarding the implementation of policies and procedures required to comply with Security Rule standards, implementation specifications or other requirements.	Required

		documented and are implemented in accordance with this subpart.		
Security	Documentation	§164.316(b)(1): (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record or the action, activity, or assessment.	Does the entity have policies and procedures to maintain written policies and procedures related to the security rule and written documents of (if any) actions, activities, or assessments required of the security rule? Obtain and review policies and procedures regarding the maintenance of policies and procedures. Obtain and review documentation demonstrating that policies and procedures are being maintained. Obtain and review written documentation demonstrating the entity's action, activity or assessment that is required by the Security Rule. Evaluate and determine if such implementation is in accordance with related policies and procedures.	Required
Security	Documentation – Time Limit	§164.316(b)(2)(i): Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Does the entity have policies and procedures in place regarding the retention of required documentation for six (6) years from the date of its creation or the date when it last was in effect? Obtain and review documentation of policies and procedures for compliance with retention requirements. Obtain and review documentation demonstrating that policies and procedures are being maintained for six (6) years from the date of its creation or the date when it last	Required

			was in effect. Obtain and review documentation demonstrating that an action, activity, or assessment is being maintained for six (6) years from the date of its creation or the date when it last was in effect. Evaluate and determine if such implementation is in accordance with related policies and procedures.	
Security	Documentation-Availability	§164.316(b)(2)(ii): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Does the entity have policies and procedures in place requiring that documentation be made available to the workforce members responsible for implementing applicable Security Rule policies and procedures? Obtain and review documentation of policies and procedures regarding the availability of documentation. Obtain and review documentation demonstrating that Security Rule policies and procedures are made available to the workforce members responsible for implementing the pertaining procedures. Evaluate and determine if implementation is in accordance with related policies and procedures.	Required
Security	Documentation – Updates	§164.316(b)(2)(iii): Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	Does the entity have policies and procedures in place to perform periodic reviews and updates to Security Rule policies and procedures? Obtain and review policies and procedures regarding documentation reviews and updates.	Required

			Obtain and review documents demonstrating that policies and procedures are reviewed and updated on a periodic basis. Evaluate and determine if such implementation is in accordance with related policies and procedures.	
Breach	Definitions: Breach – Risk Assessment ~~of Breach~~	§164.402 ~~–~~ Definitions : Breach - Risk Assessment. Breach means the acquisition, access, use, or disclosure of ~~protected health information~~PHI 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~~PHI. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable,	~~Inquire of management as to whether a risk assessment process exists to determine significant harm in a breach.~~ §164.402 Definitions: Breach - Risk Assessment Does the covered entity have policies and procedures for determining whether an impermissible use or disclosure requires notifications under the Breach Notification Rule? Does the covered entity have a process for conducting a breach risk assessment when an impermissible use or disclosure of PHI is discovered, to determine whether there is a low probability that PHI has been compromised? If not, does the covered entity have a policy and procedure that requires notification without conducting a risk assessment for all or specific types of incidents that result in impermissible uses or disclosures of PHI? Obtain and review policies and procedures regarding the process for determining whether notifications must be provided when there is an impermissible acquisition, access, use, or disclosure of PHI. If the entity does not have a policy and	~~N/A~~

		demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the PHI or to whom the disclosure was made; (iii) Whether the PHI was actually acquired or viewed; and (iv) The extent to which the risk to the PHI has been mitigated.	procedure that treats all potential breaches as requiring notifications without conducting a risk assessment, review the covered entity's risk assessment policies and procedures. Evaluate whether they require the covered entity to consider at least the following four factors: (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification (ii) The unauthorized person who used the PHI or to whom the disclosure was made (iii) Whether the PHI was actually acquired or vie (iv) The extent to which the risk to the PHI has been mitigated. Obtain a list of risk assessments, if any, conducted within the specified period where the covered entity determined there was a low probability of compromise to the PHI. Use sampling methodologies to select documentation of risk assessments to assess whether the risk assessments were completed in accordance with §164.402(2). Obtain a list of risk assessments, if any, conducted within the specified period where the covered entity determined that the PHI was compromised and notification were required under 164.404-164.408. Use sampling methodologies to select documentation of risk assessments to assess whether the risk assessments were completed in accordance with §164.402(2).	
Breach	Definitions: Breach -	§164.402 - Definitions: Breach	§164.402 - Definitions: Breach Exceptions -	

	exceptions Unsecured PHI	Exceptions - Unsecured PHI Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI. (1) Breach excludes: (i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part. (ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part. (iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or	Unsecured PHI Did the covered entity or business associate determine that an acquisition, access, use or disclosure of protected health information in violation of the Privacy Rule not require notifications under §§164.404-164.410 within the specified period? • If yes, did the covered entity or business associate determine that one of the regulatory exceptions to the definition of breach at §164.402(1) apply? If yes, obtain documentation of such determination. Use sampling methodologies to select and review documentation that such were completed in accordance with §164.402. • If yes, did the covered entity or business associate determine that the breach did not require notification, under §§164.404-410, because the PHI was not unsecured PHI, i.e., it was rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in the applicable guidance? If yes, obtain and review documentation. Use sampling methodologies to select and review documentation that such were completed in accordance with §164.402.	

		business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated. Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.		
Breach	~~Notification~~Notice to Individuals	§164.404 ~~–~~ (a)(1) 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	~~Inquire of management as to whether a process exists~~§164.404(a)(1) Notice to Individuals Does the covered entity have policies and procedures for notifying individuals ~~within the required time period. Obtain and review key documents that outline the process for notifying individuals of~~	~~N/A~~

		disclosed as a result of such breach. (2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	~~breaches~~ of a breach of their protected health information. Obtain and review a list of breaches, if any, in the specified period involving 500 or more individuals. Obtain and review documentation of notifications provided to the affected individuals. Determine whether notifications were provided to individuals consistent with the requirements in §164.404(a)(1).	
Breach	Timeliness of Notification	§~~164.404 - Notice to Individuals~~ 164.404(b) Timeliness of Notifications. 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 of a breach.	~~Inquire of management as to whether a process exists for notifying~~§164.404(b) Timeliness of Notifications Were individuals notified of breaches within the required time period~~.~~? Inquire of management. Obtain and review ~~key documents that outline the process~~the policies and procedures for notifying individuals of breaches~~. Verify, if any breaches have occurred, that individuals were notified within 60 days~~ and determine whether such policies and procedures are consistent with §164.404, including providing notification without unreasonable delay and in no case later than within 60 days of discovery of a breach.	~~N/A~~

			Obtain and review a list of breaches, if any, in the specified period and documentation indicating the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for delay in notification to determine whether all individuals were notified consistent with §164.404(a), (b).	

~~Breach~~	~~Methods of Individual Notification~~	~~§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 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~~	~~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 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.~~	~~N/A~~

		~~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.~~		
Breach	Content of Notification	§164.404 (c)(1)~~Elements~~ Content of ~~the~~Notification. The notification required by paragraph (a)	~~Inquire of management to determine if there is~~§164.404(c)(1) Content of Notification	~~N/A~~

		of this section shall include, to the extent possible: (A)~~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~~A description of the types of unsecured protected health information that were involved in the breach (~~Such~~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~~Any steps the individual should take to protect themselves from potential harm resulting from the breach; (D) ~~a~~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~~Contact procedures for individuals to ask questions or learn additional information, which ~~should~~shall include a toll-free telephone number, an email address, ~~website~~Web site, or postal address. (2) The notification required by paragraph (a) of this section shall be written in plain language.	Does the covered entity have policies and procedures for providing individuals with notifications that meet the content requirements of §164.404(c)? Inquire of management; obtain and review policies and procedures. Evaluate if the specifications at §164.404(c) are met. Inquire of management whether the covered entity has used a standard template or form letter for notification to individuals for all breaches or for specific types of breaches. If the covered entity has used a standard template or form letter for breach notification~~.~~ ~~Verify that, if any breaches have occurred, the notification to the individuals included the~~, obtain and review the document. Evaluate whether it includes this section's required elements ~~of this section~~. Obtain and review a list of breaches, if any, in the specified period and documentation of written notices sent to affected individuals for each breach. Use sampling methodologies to select notifications sent to individuals to be reviewed and verify that the notices include the elements required by §164.404(c).	
Breach	Methods of Notification	§164.404(d) Methods of Notification. The notification required by paragraph (a) of this section shall be provided in the following form:	§164.404(d) Methods of Notification Does the covered entity have policies and procedures for notifying an individual, an individual's next of kin, or a personal	

		(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 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 is required. The notification may be provided in one or more mailings as information is available. (2) Substitute notice. In the case in which 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 substitute form of notice reasonably 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 in which 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.	representative of a breach? Inquire of management. Obtain and review the covered entity's policies and procedures for notifying individuals, next of kin, or personal representatives of a breach to determine whether they are consistent with §164.404(d), including the following: • Do the policies and procedures provide that notice will be provided by first-class mail unless the individual has agreed to receive an electronic notice? If there is a process for individuals to agree to receive electronic notice, is there also a process to address circumstances where an individual withdraws such agreement? • Do the policies and procedures provide that the covered entity will send the notification to the next of kin or personal representative where the covered entity has knowledge that the individual is deceased and has the address of the next of kin or personal representative? • Do the policies and procedures address the provision of substitute notice consistent with §164.404(d)(2), including: o Alternative means for providing notification to individuals if there is insufficient or out-of-date contact information for fewer than 10 individuals o If insufficient or out-of-date contact information for 10 or more individuals - Posting a conspicuous notice on the home page of the covered entity's web site or publishing conspicuous notices in major print or broadcast media in the geographic area(s)	

		(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 unsecured 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.	where the affected individuals likely reside -Establishing a toll-free phone number that remains active for at least 90 days. Did the covered entity determine that there were any breaches within the specified period that required substitute notice? Obtain and review documentation of substitute notices: 1. If insufficient or out-of-date contact information for fewer than 10 individuals, documentation of notice provided by alternative means, such as a log of telephone call 2. if insufficient or out-of-date contact information for 10 or more individuals, documentation of a conspicuous posting on the home page of the covered entity's web site or a copy of conspicuous notices in major print or broadcast media and documentation of a toll-free phone number that remained active for at least 90 days. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.404.	
Breach	Notification to the ~~media~~Media	§164.406(a) Notification to the Media. For a breach of unsecured ~~protected health information~~PHI involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. (b)Except as provided in §164.412, a	~~Inquire of management as to whether a process exists~~§164.406(a) Notification to the Media Does the covered entity have policies and procedures for notifying media outlets ~~for breaches of more than 500 individuals' PHI and compare it to established performance criteria. Verify if any breaches of unsecured PHI have involved more than 500 individuals and~~	~~N/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 of a breach. (c) The content of the notification required by paragraph (a) of this section shall meet the requirements of §164.404(c).	~~have~~of breaches affecting more than 500 residents of a State or jurisdiction? Obtain and review policies and procedures. Evaluate whether the specifications at §164.406 are met. Obtain and review a list of breaches, if any, in the specified period affecting more than 500 residents of a State or jurisdiction. Obtain and review documentation to verify that the media notifications included the elements required ~~notification of media outlets.~~ by §164.406.	
Breach	Notification to the Secretary	§164.408 Notification to the Secretary. (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~~except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS ~~web~~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	~~Inquire of management as to whether there have been any breaches of unsecured PHI and verify that~~§164.408 Notification to the Secretary Does the covered entity have policies and procedures for notifying the Secretary ~~was notified. Verify if any~~of breaches ~~of unsecured PHI have involved~~involving 500 or more ~~than 500 individuals and have required contemporaneous notification to~~individuals? Does the covered entity have policies and procedures for notifying the Secretary~~. Verify if any~~ of breaches ~~of unsecured PHI have involved~~involving less than 500 individuals ~~and have required annual notification through the HHS website~~? Obtain and review policies and procedures. Evaluate whether the specifications at §164.408 are met. Obtain and review a list of breaches, if any, in	~~N/A~~

		~~occurring~~discovered during the preceding calendar year, in ~~a~~the manner specified on the HHS ~~web~~Web site.	the specified period involving 500 or more individuals. Obtain and review documentation of notifications provided to the Secretary. Determine whether contemporaneous notifications were provided to the Secretary consistent with the requirement in §164.408. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.408. Obtain and review a list of breaches, if any, in the specified period involving fewer than 500 individuals. Obtain and review documentation of notifications provided to the Secretary . Evaluate whether the notifications were provided to the Secretary within 60 calendar days of the end of the calendar year in which the breach was discovered, consistent with the requirement in §164.408. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.408.	
Breach	Notification by a ~~business~~Business ~~associate~~Associate	§ 164.410~~(a)~~ Notification by a Business Associate. (a) Standard. (1) General Rule. -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 (a) (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	~~Inquire of management as to whether there have been~~§ 164.410 Notification by a Business Associate Did the business associate or subcontractor determine that there were any breaches of unsecured PHI ~~for a~~within the specified period? If yes, obtain copies of the notification(s) sent by the business associate ~~and verify that~~(or subcontractor) to the covered entity ~~was~~	~~N/A~~

		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 disclosuredisclosed during the breach. (2) A business associate shall provide the covered entity with any other available 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.	notified. Obtain the standard business associate agreement to verify that the breach and notification(or business associate for breaches by subcontractors). Evaluate whether the business associate or subcontractor sent the notifications consistent with the requirements at §164.410. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements are included in the agreement. required by §164.410.	
Breach	Law	§164.412	Inquire of management as to how	N/A

	~~enforcement~~Enforcement ~~delay~~Delay	Law Enforcement Delay. 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.	~~notifications are delayed in case of~~§164.412 Law Enforcement Delay Does the covered entity or business associate have policies and procedures regarding how the covered entity or business associate would respond to a law enforcement statement that a notice or posting would impede a criminal investigation or damage national security? Has the covered entity or business associate delayed notification of a breach of unsecured PHI pursuant to such a law enforcement ~~requests. Obtain~~statement? If yes, obtain and review documentation of ~~the process to delay notifications in case of~~any such law enforcement ~~requests~~statement. Evaluate whether the covered entity or business associate acted in accordance with §164.412. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.412.	
Breach	Administrative Requirements	§164.414(a) Administrative Requirements. A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to 45 CFR Part 164, Subpart D ("the Breach Notification Rule"). [Training, complaints to the covered entity, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures, and	164.414(a) Administrative Requirements: Has the covered entity adequately implemented the required 164.530 provisions as they relate to the Breach Notification Rule? Inquire of management.	

		documentation]		
Breach	Burden of Proof	§164.414~~ - Administrative requirements and burden~~(b) 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~~the subpart or that the use or ~~disclosures~~disclosure did not constitute a breach as defined at §164.402.~~ See §164.530 for definition of breach.~~	~~Inquire~~§164.414(b) Burden 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.~~ proof	~~N/A~~
Privacy	Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes	§ 164.502(a)(5)(i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan: (A) Except as provided in paragraph (a)(5)(i)(B) of this section: (1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan,	Does the health plan use or disclose for underwriting purposes, "Genetic Information" as defined at § 160.103, including family history? Inquire of management. Obtain and review all underwriting policies and procedures (for example, published and unpublished underwriting guidelines currently used by underwriting staff, including manuals and training materials). Evaluate whether the underwriting policies are consistent with the established performance criterion.	

		coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and (4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. (B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy. From § 160.103 Definitions. Genetic information means: (1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about: (i) The individual's genetic tests; (ii) The genetic tests of family members of the individual; (iii) The manifestation of a disease or disorder in family members of such individual; or (iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. (2) Any reference in this subchapter to genetic information		

		concerning an individual or family member of an individual shall include the genetic information of: (i) A fetus carried by the individual or family member who is a pregnant woman; and (ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology. (3) Genetic information excludes information about the sex or age of any individual. (ii) Genetic services means: (1) A genetic test; (2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) Genetic education. Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.		
Privacy	Deceased individuals	§164.502~~ Uses and disclosures of protected health information: general rules~~(f) Standard: Deceased individuals: A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual. From § 160.103 Definitions. Protected health information means individually identifiable health information: (1) Except as provided in	Do the covered entity's policies and procedures protect the deceased individual's PHI consistent with the established performance criterion? 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~~policies and procedures regarding use	~~N/A~~

		paragraph (2) of this definition.[….] (2) Protected health information excludes individually identifiable health information: [….] (iv) Regarding a person who has been deceased for more than 50 years.	and disclosure of deceased individuals' PHIs. Evaluate whether the policies and procedures are consistent with the established performance criterion.	
Privacy	Personal representatives	§164.502~~ - Uses and disclosures of protected health information: general rules §164.502(g)(2) -~~(g)(1) Standard: Personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter. §164.502(g)(2) Implementation specification: adults and emancipated minors: 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) ~~-~~ Implementation specification: unemancipated minors: 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	Do the policies and procedures provide for the treatment of an authorized person as a personal representative? Inquire of management ~~as to whether requirements with respect to~~how the entity recognizes 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~~for an individual for compliance with HIPAA Rule requirements. Obtain and review policies and procedures for the recognition and treatment of a personal representative. Evaluate whether the policies and procedures are consistent with the established performance criterion. For example, do the policies and procedures address how the covered entity determines whether a person has authority to act on behalf of the individual? How do the policies and procedures address minors? The deceased? Obtain and review a sample of personal representatives recognized by the entity. Evaluate whether the personal representative has been recognized and treated in a manner consistent with the established performance criterion and the entity established policies	~~N/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~~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~~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~~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~~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,	and procedures. Obtain and review a sample of requests for persons to be recognized as personal representatives for individuals where the entity has not recognized the person as a personal representative. Evaluate whether the decision to not recognize the person as a personal representative was consistent with the established performance criterion and entity established policies and procedures. Evaluate whether the person has been treated consistent with the established performance criterion and the entity established policies and procedures.	

		or ~~provide access~~ in accordance with §164.524 provide access to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; (~~b~~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 §164.524 provide access to , protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and (~~c~~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~~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(g)(4) Implementation specification: Deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, 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) (5) Implementation specification: Abuse, neglect, endangerment situations. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if: (i) The covered entity has a reasonable belief that: (A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or (B) Treating such person as the personal representative could endanger the individual; and (ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.		
Privacy	Confidential communications	§164.502(h) Standard: Confidential communications: 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) Standard: Confidential communications requirements: (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by	How does the entity provide for and accommodate requests by individuals for confidential communications? Inquire of management how the entity handles requests for confidential communications by individuals. Obtain and review policies and procedures regarding requests for confidential communications. Evaluate whether the policies and procedures are consistent with	

		individuals to receive communications of protected health 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. §164.522(b)(2) Implementation specifications: Conditions on providing confidential communications: (i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing. (ii) A covered entity may condition the provision of a reasonable accommodation on: (A) When appropriate, information as to how payment, if any, will be handled; and (B) Specification of an alternative address or other method of contact. (iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis. (iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.	the established performance criterion. Obtain and review a sample of confidential communications requests made by individuals. Evaluate whether the requests were evaluated and accepted or denied consistent with the established performance criterion and the entity established policies and procedures. Obtain a review a sample of communications to individuals for which a confidential communication request was accepted. Evaluate whether the communication was conducted consistent with the established performance criterion and the entity established policies and procedures.	

Privacy	Uses and disclosures consistent with notice	§164.502(i) Standard: Uses and disclosures consistent with notice: 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~~A)-(~~c~~C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.	Are uses and disclosures made by the covered entity consistent with its notice of privacy practices? Inquire of management ~~as to~~ whether uses and disclosures of PHI are consistent with the entity's notice~~.~~ of privacy practices. Obtain and review ~~the process and evaluate the content in relation to the specified criteria to determine if the process for~~policies and procedures regarding uses and disclosures ~~is~~. Evaluate whether the uses and disclosures of PHI are consistent with the entity's notice of privacy practices.	~~N/A~~
Privacy	Disclosures by whistleblowers	§164.502(j)(1) Disclosures by whistleblowers: 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) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the	~~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~~Are whistleblower policies and procedures consistent with the requirements of this performance criterion? Obtain and review documentation of disclosures by a workforce member not otherwise permitted by the Privacy Rule that the entity determined to meet the requirements of this standard.	~~N/A~~

		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~~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.		
Privacy	Disclosures by workforce members who are victims of a crime	§164.502(j)(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).	~~Inquire of management as to whether a process exists to permit certain~~How has the covered entity ensured that disclosures by a workforce member related to his or her status as a victim of a crime are consistent with the rule? Inquire of management how the entity identifies and treats 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 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~~. Obtain and review policies and procedures	~~N/A~~

			related to disclosures of PHI by workforce members who are ~~crime~~ victims of a crime. Evaluate whether disclosures are treated consistent with the established performance criterion and the entity established policies and procedures.	
~~Privacy~~	~~Confidential communications~~	~~§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.~~	~~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.~~	~~N/A~~

Privacy	Business associate contracts	§164.504~~ - Uses and disclosures: Organizational requirements~~(e)(1) Standard: Business associate contracts. (i) The contract or other arrangement ~~between the covered entity and the business associate~~ required by § 164.502(e)(2) must meet the requirements of ~~the following, as applicable. -~~ paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible. (iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible. (2) Implementation specifications:	~~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~~Does the covered entity enter into business associate contracts as required? Do these contracts contain all required elements? Inquire of management how the entity identifies and engages business associates. Obtain and review policies and procedures related to the identification of business associates and the creation and establishment of business associate agreements. ~~Obtain and review formal or informal~~Evaluate whether the policies and procedures ~~and evaluate the content relative to the specified criteria for identifying whether a~~accurately identify business associates and establish business associate agreements consistent with the established performance criterion established performance criterion. Technical Assistance: if available, review the entity's template business associate agreement ~~is required. Verify whether the agreement limits uses and disclosures to those that are permitted by the standard. Obtain and review a business associate agreement and evaluate the content relative to the specified criteria~~and provide technical assistance as to its contents. Obtain and review a sample of business associate agreements. Evaluate whether the	~~N/A~~

		Business associate contracts. -A contract between the covered entity and a business associate must: (i) Establish the permitted and required uses and disclosures of ~~such~~protected health 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~~ , as provided in paragraph (e)(4) of this section; 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 and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract; (C) Report to 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~~	agreements are consistent with the established performance criterion entity-established policies and procedures. Inquire of management as to whether any business associate arrangements involved onward transfers of PHI to additional business associates and subcontractors. If yes, review a sample of business associate agreements between the covered entity and such business associates for provisions requiring subsequent BAs/subcontractors to provide adequate assurances. Has the covered entity come into the knowledge of a pattern or practice of the business associate that constituted a material breach of violation of the BA's obligation? If so, obtain documentation of covered entity response and evaluate against the established performance criterion established performance criterion. Use of sampling procedures may be appropriate. Obtain and review documentation of reports from the business associate to the covered entity of any uses or disclosures not provided for in its contract, and the covered entity response.	

		~~agents~~, including ~~a subcontractor, to whom it provides~~breaches of unsecured protected health information ~~received from, or created or received by the business associate on behalf of, the covered entity agrees~~as required by § 164.410; (D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree 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~~ (H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation. (I) 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 (J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. (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. (3) Implementation specifications: Other arrangements. (i) If a covered entity and its business associate are both governmental entities: (A) The covered entity may comply with this ~~section~~ paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section~~.~~ and § 164.314(a)(2), if applicable. (B) The covered entity may comply with this ~~section~~paragraph and § 164.314(a)(1), if applicable, 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 paragraph (e)(2) of this section~~.~~ and § 164.314(a)(2), if applicable. (ii) If a business associate is required by law to perform a function or ~~activities~~activity 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~~paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such ~~attempts~~attempt fails, documents the attempt and the reasons that such assurances cannot be obtained. (iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate. (iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the		

		business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable. (4) Implementation specifications: Other requirements for contracts and other arrangements. (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary: (A) For the proper management and administration of the business associate; or (B) To carry out the legal responsibilities of the business associate. (ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if: (A) The disclosure is required by law; or (B)(1) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and		

		(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached. (5) Implementation specifications: Business associate contracts with subcontractors. The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.		
Privacy	Requirements for group health plans	§164.504 ~~- Uses and disclosures: Organizational requirements~~ (f)(1) Standard: Requirements for group health plans. (i) Except as provided under paragraph (f)(1)(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~~Except as prohibited by § 164.502(a)(5)(i), the group health plan, or a health insurance issuer or ~~HMP~~HMO with respect to the group health plan, may disclose summary health information to	~~Inquire of management as to whether the~~Do group health plan documents restrict the use and disclosure of PHI ~~by~~to the plan sponsor~~.~~ ? Obtain and ~~review a sample of~~evaluate group health plan documents~~. Verify~~ to determine if they restrict the use and disclosure of PHI ~~by~~to the plan sponsor ~~is restricted. Verify what information the sponsor does obtain and how it is used~~consistent with the established performance criterion.	~~N/A~~

		the plan sponsor, if the plan sponsor requests the summary health information for ~~the purpose~~purposes of: (A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or (B) ~~Modify~~Modifying, 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~~HMO offered by the plan. (2) Implementation specifications: Requirements for plan documents. The plan documents of the group health plan must be amended to incorporate provisions to: (i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart. (ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to: (A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law; (B) Ensure that any agents to whom it provides protected health information		

		received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information; (C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor; (D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware; (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 the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart; (I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or		

		destruction of the information infeasible; and (J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established. (iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must: (A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description; (B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and (C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph. (3) Implementation specifications: Uses and disclosures. A group health plan may: (i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section; (ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health		

		information to the plan sponsor except as permitted by this paragraph; (iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and (iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.		
Privacy	Requirements for a covered entity with multiple covered functions	§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.	~~Inquire of management as to whether the entity has~~For entities that perform multiple covered functions, are uses and ~~if the use and disclosure~~disclosures of PHI ~~is~~ only for the purpose related to the appropriate ~~function~~functions being performed~~.~~ ? Inquire of management. Obtain and ~~review formal documentation and evaluate the content in relation to the specified criteria for restricting the use and disclosure~~evaluate whether the policies and procedures restrict the uses and disclosures 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~~	~~N/A~~

			has been approved and updated on a periodic basis.	
Privacy	Permitted uses and disclosures	§164.506(a) - 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 (3 164.508(a)(2) through (4) or that are prohibited under § 164.502(a)(5)(i), 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.	Inquire of management as to whether a process existsDo policies and procedures exist 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? Inquire of management. Obtain and review policies and procedures regarding 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 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 requirementsor health care operations.	N/A
Privacy	Consent for uses and disclosures	§164.506 – Uses(b) - Standard: Consent for uses and disclosures to carry out treatment, payment, or health care	Inquire of management as to whetherDoes the entity has determined that obtainingobtain the individual's	N/A

		~~operations~~ permitted. §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 ~~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~~for uses and disclosures? Obtain samples of completed consents, if any, and patient intake materials and review to determine if its use is consistent with the established performance criterion.	

~~Privacy~~	~~Obtaining Authorization as Required for Internal Use and Disclosure of Protected Health Information~~	~~§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)~~	~~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.~~	~~N/A~~

		~~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 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.~~		
Privacy	Authorizations for uses and disclosures is required	~~§164.508 - Uses and disclosures for which an authorization is required~~ §164.508(a)(1) Authorization required:	~~Inquire of management as to whether formal or informal~~What policies and procedures exist for obtaining a valid	~~N/A~~

		General rule. 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~~ §164.508(a)(2) Authorization required: Psychotherapy notes. (i) 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~~psychotherapy notes, except: (i) To carry out the following treatment, payment, or health ~~information for marketing.~~ care operations: (A) Use by the originator of the psychotherapy notes for treatment; (B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in	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~~ when required? Do policies and procedures exist to determine when authorization is required? Obtain and review against the established performance criterion the policies and procedures for obtaining a valid authorization as required by the standard: -Documentation of covered entity policy and procedures -Documentation that a standard covered entity authorization, if any, is valid Obtain and evaluate a sample of authorizations obtained to permit disclosures for consistency with the established performance criterion and entity-established policies and procedures. For providers only: obtain and review all relevant patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any, to assess whether the provider's practice is to use a consent when an authorization would be required for any use or disclosure of information pursuant to the consent.	

		group, joint, family, or individual counseling; or (C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and (ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i). §164.508(a)(3) Authorization required: Marketing. (i)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, except if the communication is in the form of: (A) A face-to-face communication made by a covered entity to an individual; or (B) a promotional gift of nominal value provided by the covered entity. (ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved. §164.508(a)(4) Authorization required: Sale of protected health information. (i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any		

		disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart. (ii) Such authorization must state that the disclosure will result in remuneration to the covered entity. §164.508(b)(1) Valid authorizations. (i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as 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 required by this section. §164.508(b)(2) Defective authorizations. An authorization is not valid, if the document submitted has any of the following defects: (i) The 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.		

Privacy	Compound authorizations -- Exceptions	§164.508(b)(3) Compound authorizations. -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 or another research study~~, including another~~. This exception includes combining an authorization for the use or disclosure of protected health information for ~~such research or a~~a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with consent to participate in ~~such research;~~ research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization. (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~~;~~ .	~~Inquire of management as to whether~~Does the covered entity ~~uses~~use or ~~discloses~~disclose PHI for the purpose of research, conducts research, provides ~~research and/or~~ psychotherapy services, ~~or~~and 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~~sample of used compound authorizations, if any. Evaluate such authorizations ~~and evaluate the content~~ in relation to the ~~specified criteria to determine if the compound authorizations are appropriate.~~ established performance criterion: -Compound authorizations for the same research study -difference between conditioned and unconditioned components -Use or disclosure of psychotherapy notes and -Any other prohibition required under the established performance criterion	~~N/A~~

		(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. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.		
Privacy	Prohibition on conditioning of authorizations	§164.508(b)(4) Prohibition on conditioning of authorizations. 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 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	~~Inquire of management as to when~~Does the covered entity ~~can condition the provision to an individual of treatment, 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~~condition treatment, payment, enrollment, or eligibility ~~is conditioned~~on receipt of an authorization? If so, does one of the limited exceptions apply? Obtain and review policies and procedures related to seeking authorizations from individuals. Obtain and review a sample of conditioned	~~N/A~~

		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~~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.	authorizations to assess whether the exceptions listed in the ~~documents: -Evidence of provider/payer health plan conditions~~ established performance criterion have been applied consistent with its requirements.	
Privacy	~~Limited uses and disclosures when the individual~~Uses and Disclosures for which an Authorization is ~~not present~~Required – Documentation and Content	§~~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~~164.508(b)(6) Documentation. A covered entity must document and retain any signed authorization under this section as required by §164.530(j). §164.508(c) Implementation	~~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~~Does the covered entity document and retain signed, valid authorizations? Obtain and review a sample of authorizations used as the basis for making uses and disclosures to determine if the authorizations are valid.	~~N/A~~

		specifications: Core elements and requirements. (1) Core elements. A valid authorization under this section must contain at least the following elements: (i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion. (ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure. (iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure. (iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual ~~and, if so, disclose only~~ initiates the authorization and does not, or elects not to, provide a statement of the purpose. (v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of 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~~for research, including for the creation and maintenance of a research database or research repository. (vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided. §164.508(c)(2) Required Statements. 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 and either: (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 from 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.		

Privacy	Use and Disclosure for Facility Directories; Opportunity to Object	§164.510(a)~~(1)~~ Standard: Use and disclosure for facility directories. (1) Permitted uses and disclosure. 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~~Use or disclose 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. (2) Opportunity to object. 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.	~~Inquire of management as to whether~~Does the entity ~~maintains~~maintain a directory of individuals in its facility~~.~~? Obtain and review policies and procedures that address determining if the individual has objected to uses and disclosures for facility directories and for documenting such determination. Obtain and review a sample of the 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~~that exists on the specified date and related documentation of individual objections. Evaluate the content against documentation of individual objections and against the listed content criteria.	~~N/A~~

Privacy	Uses and Disclosures for Facility Directories in Emergency Circumstances	§164.510(a)(3) Emergency circumstances. -(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, if such disclosure is: (A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and (B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment. (ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.	~~Inquire of management as to whether a process exists~~Do policies and procedures exist to use or disclose PHI for the facility directory ~~due to an~~in emergency ~~treatment.~~ circumstances? Obtain and review the ~~process~~policies and procedures 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~~circumstance.	~~N/A~~
Privacy	Permitted uses and ~~disclosers~~disclosures	§164.510(b)~~(1)~~ Standard: Uses and disclosures for involvement in the individual's care and notification purposes (1) Permitted uses and disclosures. -(i) A covered entity may, in accordance with paragraphs (b)(2) , (b)(3), or (b~~3~~)(5) 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, the protected health information directly relevant to such person~~'~~'s involvement	~~Inquire of management as to what the process is~~What policies and procedures exist 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.	~~N/A~~

		with the individual[1]'s health care or payment related to the individual[1]'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), (b) (3), (b)(4), or (~~4~~ b)(5) of this section, as applicable.		
Privacy	Uses and disclosures with the individual present	§164.510(b)~~(2)~~ Standard: Uses and disclosures for involvement in the individual's care and notification purposes (2) Uses and disclosures with the individual present. 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 on the exercise of	~~Inquire of management as to how~~Under what circumstances does the covered entity ~~discloses~~disclose PHI to persons involved in the individual's care when the individual is present~~, and whether the entity can disclose~~? Obtain and review policies and procedures for determining or inferring individual agreement or lack of objection to disclosure of 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~~	~~N/A~~

		professional judgment, that the individual does not object to the disclosure.		
Privacy	Limited uses and disclosures when the individual is not present	§164.510(b)(3) Limited uses and disclosures when the individual is not present. 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 care or payment related to the individual's health care or needed for notification purposes. 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.	Do policies and procedures exist for disclosing only information relevant to the person's involvement in the individual's health care when the individual is not present and in related situations? Obtain and review the policies and procedures used for disclosing only information relevant to the person's involvement with the individual's health care.	
Privacy	Uses and disclosures for disaster relief purposes	§164.510(b)~~(4)~~ Standard: Uses and disclosures for involvement in the individual's care and notification purposes (4) Uses and disclosures for disaster relief purposes. 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	~~Inquire of management as to whether a process exists~~Do policies and procedures exist for disclosing PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts~~.~~ ? Obtain and review policies and procedures ~~and evaluate the content in relation to the relative specified criteria related to~~	~~N/A~~

		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~~paragraphs (b)(2) ~~and~~ , (b) (3) or (b)(5) of this section apply to such uses and ~~disclosure~~disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.	~~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~~in relation to such use or disclosure.	
Privacy	~~Opportunity to Object~~Uses and disclosures when the individual is deceased	~~§~~164.510 ~~–~~(b) Standard: Uses and disclosures ~~requiring an opportunity~~ for involvement in the individual ~~to agree or to object §164.510(a)(2) A covered health care provider must inform an individual of the~~'s care and notification purposes (5) Uses and disclosures when the individual is deceased. If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, 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~~	~~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~~Does the covered entity disclose the PHI of deceased individuals in accordance with the established performance criterion? Obtain and review policies and procedures related to documenting the individual's prior expressed preference and relationship of family members and other persons to the individual's care or payment for care, consistent with the established performance criterion. Note: any information that would otherwise constitute PHI of a decedent under §160.201 ceases to be PHI 50 years after the death of	~~N/A~~

		~~disclosures permitted by paragraph (a)(1) of this section~~of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.	the decedent.	

~~Privacy~~	~~Disclosures for judicial and administrative proceedings~~	~~§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~~	~~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 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.~~	~~N/A~~

		~~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 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.~~		

~~Privacy~~	~~Uses and disclosures for research purposes~~	~~§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 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~~	~~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: -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.~~	~~N/A~~

		~~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 . . .~~		

~~Privacy~~	~~Uses and disclosures for research purposes~~	~~§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~~	~~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 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~~	~~N/A~~

		~~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 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~~	~~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.~~	

		~~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.~~		
Privacy	Uses and disclosures required by law	§164.512(a)(1) - A covered entity may use or disclose protected health information to the extent that such use or	~~Inquire of management as to whether the requirements to~~Does the covered entity use ~~or disclose PHI required by law~~	~~N/A~~

		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.	~~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.~~ and disclose PHI pursuant to requirements of other law? If so, are such uses and disclosures made consistent with the requirements of this performance criterion as well as the applicable requirements related to victims of abuse, neglect or domestic violence, pursuant to judicial and administrative proceedings and law enforcement purposes of this section? Obtain and review policies and procedures ~~and evaluate the content in relation to the specified criteria~~ for uses and disclosures required by law.	
Privacy	Uses and disclosures for public health activities	§164.512(b)~~(1) -~~ Standard: Uses and disclosures for public health activities. (1) Permitted uses and disclosures. A covered entity may use or 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	~~Inquire of management as to whether a process is in place specifying~~Are policies and procedures in place that specify how the covered entity uses or disclosures PHI for public health activities ~~for which the entity may disclose PHI.~~ consistent with this standard? Obtain and review ~~formal or informal~~ policies and ~~evaluate the content~~procedures in relation to the ~~specified criteria on~~established performance criterion regarding permitted uses and disclosures for public health activities. Obtain and review a sample of such uses~~/~~ and	~~N/A~~

		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~~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~~B) To track FDA-regulated products; (~~c~~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~~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	disclosures, to include ~~(v)~~ uses and disclosures to an employer about an individual who is a member of the workforce of the employer, and determine whether all criteria were met. ~~Auditors should refer to the established performance criteria to identify what subpart (v) includes.~~	

		who is a member of the workforce of the employer, if: (~~a~~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~~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~~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~~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 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. (vi) A school, about an individual who is a		

		student or prospective student of the school, if: (A) The protected health information that is disclosed is limited to proof of immunization; (B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and (C) The covered entity obtains and documents the agreement to the disclosure from either: (1) A parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or (2) The individual, if the individual is an adult or emancipated minor. (2) Permitted uses. If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.		
Privacy	Disclosures about victims of abuse, neglect or domestic violence	§164.512(c)~~(1) -~~ Standard: Disclosures about victims of abuse, neglect or domestic violence (1) Permitted disclosures. 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	~~Inquire of management as to~~How does the covered entity determine whether ~~disclosure~~and how to make disclosures 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~~consistent with	~~N/A~~

		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~~disclosure; or (iii) To the extent the disclosure is expressly authorized by ~~status~~statute or regulation and: (~~a~~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~~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) ~~-~~ Informing the individual. 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	this standard? Obtain and review policies and procedures. When and in what instances will 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.~~ that a disclosure has been or will be made?	

		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.		
Privacy	Uses and disclosures for health oversight activities	§164.512(d)~~(1) -~~ Standard: Uses and disclosures for health oversight activities (1) Permitted disclosures. 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) - Exception to health oversight activities. 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	~~Inquire of management as to whether~~Is PHI ~~is disclosed to the appropriate health oversight agency. Obtain and review the policy on permissible uses and disclosures. Obtain a sample of disclosures~~used or disclosed for health oversight activities consistent with the established performance criterion? Obtain and review policies and procedures for using or disclosing PHI for health oversight activities. Obtain a sample of disclosures made for this purpose and verify that the established performance criterion have been met. Regarding §164.512(d)(4), is the covered entity also a health oversight agency? If so, is PHI used for health oversight activities conducted by the covered entity? If yes, obtain and review policies and procedures for using PHI for health oversight activities conducted by the covered entity and determine whether they are consistent with the requirements of the established performance criterion.	~~N/A~~

		activity in which the 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) - Joint activities or investigations. 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) - Permitted uses. 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.	Obtain a sample of uses made for this purpose and verify that ~~criteria~~the established performance criterion have been ~~appropriately applied~~met.	
Privacy	Disclosures for judicial and administrative proceedings	§164.512(e)(1) Permitted disclosures. 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	Do policies and procedures exist related to making disclosures in the course of any judicial or administrative proceeding to limit such disclosures to those permitted by the established performance criterion? Obtain and review policies and procedures related to disclosures of PHI made pursuant to	

		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 purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances 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 party requesting such information 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	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. Elements to consider include, but are not limited 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 the established performance criterion and include, but are not limited to: -A court order requesting a response -A subpoena.	

		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 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) or (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)(v) of this section. (2) Other uses and disclosures under this section. The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.		
Privacy	Disclosures for law enforcement purposes	§164.512(f) - Standard: Disclosures for law enforcement purposes. 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	~~Inquire of management as to whether conditions for disclosure of PHI to a~~Have disclosures made by the covered entity for law enforcement ~~official are appropriate.~~ purposes been consistent with the performance criterion? Obtain and review policies and procedures	~~N/A~~

		applicable. (1) Permitted disclosures: 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) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer; (~~b~~B) A grand jury subpoena; or (~~c~~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~~	related to disclosures of PHI ~~to~~for law enforcement ~~officials.~~ purposes against the established performance criterion. Obtain and review a sample, as available, of disclosures and the corresponding court orders, subpoenas, ~~or~~ discovery requests ~~to law enforcement officials~~, etc., 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)~~ consistent with the established performance criterion.	

		~~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, or typing, samples or analysis of blood fluids or tissue.~~		
Privacy	Disclosures for law enforcement purposes - for identification and location -	§164.512(f)(2) Permitted disclosures: 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	Are disclosures made to law enforcement for identification and location purposes by the covered entity consistent with the limitations listed in the established performance criterion?	

		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 rh 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, or typing, samples or analysis of blood fluids or tissue.	Obtain and review policies and procedures related to disclosures of PHI to law enforcement officials for identification and location purposes. Obtain and review a sample of responses to law enforcement officials request for PHI for identification and location purposes and assess whether the disclosures were consistent with the established performance criterion.	
Privacy	Disclosures for law enforcement purposes-- PHI of a possible victim of a crime	See above . . . §164.512(f)(3) - Permitted disclosure: 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	Inquire of management as to whether theAre policies and procedures consistent with the established performance criterion regarding the conditions in which the covered entity may disclose PHI of a possible victim of a crime in response to a law enforcement official's request is limited to information	N/A

		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~~disclosure; or (ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that: (~~a~~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~~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~~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) -~~	~~for identification and location purposes. Obtain and review responses to each category of disclosure in response~~? Obtain and review policies and procedures related to such disclosures of PHI to law enforcement. If any, obtain and review a sample of responses 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~~was made consistent with the	

		~~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~~	established performance criterion.	

		official for law enforcement purposes is subject to paragraph (c) of this section.		
Privacy	Disclosures for law enforcement purposes-- an individual who has died as a result of suspected criminal conduct	See above§164.512(f)(4) Permitted disclosure: Decedents. 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.	Inquire of management as to whether conditions in which the entity may disclose PHI in response to 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 responseAre	N/A

			policies and procedures in place to determine when it is permitted to disclose PHI to law enforcement about an individual who has died as a result of suspected criminal conduct? Obtain and review policies and procedures related to disclosures of PHI to ~~a law enforcement official's request about a victim of crime and is permitted~~law enforcement officials that address the requirement. Obtain and review documentation of such a disclosure, if available. Elements to consider include, but are not limited to~~: Individual consent to disclose PHI.~~ , documentation of: -Whether the entity exercised professional judgment -Whether the entity believes in good faith that there was evidence of criminal conduct.	
Privacy	Disclosures for law enforcement purposes: crime on premises	~~See above~~§164.512(f)(5) Permitted disclosure: Crime on premises. A covered entity may disclose to a 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.	~~Inquire of management as to whether a process is~~Are policies and procedures in place to determine when it is permitted to disclose PHI about an individual who ~~has died to a law enforcement official.~~ may have committed a crime on the premises? Determine whether policies and procedures related to disclosures of PHI to law enforcement officials address the established performance criterion. Obtain and review a 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~~	~~N/A~~

			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, if available. Elements to consider include, but are not limited to:, documentation of: -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.	
Privacy	Disclosures for law enforcement purposes	See above§164.512(f)(6) Permitted disclosure: 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 a 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 (C) The identity, description, and location of the perpetrator of such crime.	Inquire of management as to whether a process isAre policies and procedures 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? Determine whether policies and procedures related to disclosures of PHI to law enforcement officials address the established performance criterion. Obtain and review a sample of such disclosures. Elements to consider include, but are not limited to, whether the disclosure:	N/A

		(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.	-Indicates the commission and nature of the crime~~.~~ -Includes the location of the crime or the victim(s) of the 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.~~	
Privacy	Uses and disclosures about decedents	§164.512(g) Standard: Uses and disclosures about decedents. (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~~the duties ~~or~~of 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	~~Inquire of management as to whether the process~~Are policies and procedures consistent with the established performance criterion for disclosing PHI to (1) 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~~; and (2) a funeral director? Obtain and review policies and procedures related to disclosures of PHI to coroners and medical examiners and funeral directors. Obtain and review a sample of such disclosures. Elements to consider include, but are not limited to, whether the purpose of disclosure is: ~~-Is to~~To identify a deceased person~~. -Is to~~ -To determine the cause of death.~~ -Is authorized by law. Verify disclosures~~	~~N/A~~

		protected health information prior to, and in reasonable anticipation of, the individual's death.	~~about decedents are appropriate. Elements~~ -Authorized by law. Information elements to consider include, but are not limited to~~:~~, whether the information disclosed is limited to: -Name of deceased person~~.~~ -Cause of death~~.~~ -Compliance with such law.	
Privacy	Uses and disclosures for cadaveric organ, eye or tissue donation	§164.512(h) ~~-~~ Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes. 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~~tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.	~~Inquire of management as to whether~~Is the covered entity's process for disclosing PHI to organ procurement organizations or other entities engaged in the procurement ~~is appropriate.~~ consistent with the established performance criterion? Obtain and review policies and procedures related to disclosures of PHI for purposes of cadaveric organ, eye, or tissue donation. Obtain and review a sample of disclosures of PHI to organ procurement ~~organization~~organizations to determine ~~the purpose of~~whether such disclosures~~. Based on the complexity of the entity, elements to consider include, but~~ are ~~not limited to, whether the disclosure: 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~~	~~N/A~~

			~~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.~~ consistent with the policies and procedures and the established performance criterion.	
Privacy	Uses and disclosures for research purposes -- Permitted Uses and Disclosures	§164.512(i) Standard: Uses and disclosures for research purposes (1) Permitted uses and disclosures. 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), established in accordance with7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; 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 rights and related	Does the covered entity use or disclose PHI for research purposes? Inquire of management. For entities that conduct research using or disclosing PHI, obtain and review related policies and procedures. Elements to consider include, but are not limited to, how the entity: -Obtains documentation that an alteration to a required authorization, or waiver of the authorization, has been approved by an IRB or appropriately configured privacy board -Obtains from the researchers the required representations regarding reviews preparatory to research on decedents. Verify if the entity obtained the necessary authorization and/or waiver to conduct the research. Elements to consider 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.	

		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.		

Privacy	Uses and disclosures for research purposes -- Documentation of Waiver Approval	§164.512(i) Standard: Uses and disclosures for research purposes (2) 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 or date of action - A statement identifying the institutional review board or privacy board and the date on which the alteration or waiver of authorization was approved; (ii) Waiver criteria - A statement that the institutional review board 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	Do policies and procedures exist to determine what documentation of approval or waiver is needed to permit a use or disclosure and to apply that determination? Obtain and review policies and procedures against established performance criterion. Is the entity using or disclosing PHI consistent with requirements for documentation of a waiver approval? Verify that the documentation of any 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 the criteria listed in the standard, including determination of no more than minimal risk to privacy, adequate plan to protect identifiers, adequate plan to destroy identifiers, etc.	

		study, or for other research for which the use or disclosure of protected health information would be permitted by this 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 institutional review board or privacy board, 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 institutional review board must follow the requirements of the Common Rule, including the normal review procedures or the expedited review procedures: 7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b),38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110,		

		28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45; (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 procedure 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 institutional review board or the privacy board, as applicable.		
Privacy	Uses and disclosures for specialized	§164.512(k)~~(1) -~~ Standard: Uses and disclosures for specialized government	~~Inquire of management as to whether a process is in place to determine for~~	~~N/A~~

	government functions -- Military	functions. (1) Military and veterans activities (i) Armed Forces personnel. 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~~A) Appropriate military command authorities; and (~~b~~B) The purposes for which the protected health information may be used or disclosed. (ii) Separation or discharge from military service. A covered entity that is a component of the Departments of Defense or ~~Transportation~~Homeland Security 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) Veterans. 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	~~which government functions~~Does the covered entity ~~is permitted~~ disclose PHI~~.~~ of individuals for military and veterans activities consistent with the established performance criterion? Obtain and review policies and procedures related to disclosures of PHI for purposes of military and veterans' activities. 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~~military and veterans activities. Elements to consider are, 1) whether the entity is a component of the DoD, HSA; or VA; and 2) include~~, but are not limited to,~~ whether the disclosure~~: -Is for an armed~~ relates to: - Armed force personnel~~. -Is for a separated~~ - Separated or discharged military service personnel~~. -Is for a~~ - A veteran~~. -Is for a foreign~~ - Foreign military personnel.~~ -Verify disclosures of PHI are for appropriate government functions~~ . Elements to consider include, but are not limited to: -Whether the 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 personnel.~~	

		Secretary of Veterans Affairs. (iv) Foreign military personnel. 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 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.~~		
Privacy	Uses and disclosures for specialized government functions -- National Security and intelligence activities	~~See above. §164.512(k)(5) Correctional institutions and other law enforcement custodial situations. (i)~~ §164.512(k)(2) National security and intelligence activities. 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~~	~~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~~How would the covered entity respond	~~N/A~~

		~~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~~	to a request for PHI from Federal officials for intelligence and other national security activities~~ authorized by the National Security Act. Verify~~? Obtain and review policies and procedures related to 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~~for national security purposes.	

		~~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 improve administration and management relating to the covered functions of~~		

		~~such programs~~to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U. S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).		
Privacy	Uses and disclosures for specialized government functions -- Protective Services	~~See above~~§164.512(k)(3) Protective services for the President and others. 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 for the conduct of investigations authorized by 18 U.S.C. 871 and 879.	~~Inquire of management as to whether a process is in place to determine for what protective services~~How would the covered 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~~respond to a request for PHI from Federal officials for the provision of protective services ~~to the President. -For other authorized persons. -For~~or the conduct of certain investigations ~~authorized by 18 U.S.C 871 and 879. Verify~~? Obtain and review policies and procedures related to 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~~.	~~N/A~~

Privacy	Uses and disclosures for specialized government functions -- Medical Suitability Determinations	~~See above~~§164.512(k)(4) Medical suitability determinations.- 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.	~~Inquire of management as to whether a process is in place to determine the purpose for disclosing PHI to the Department of State (DOS).~~ Is the covered entity a component of the Department of State? If yes, does the covered entity have policies and procedures consistent with the established performance criterion to use and disclose PHI for the purposes described in the established performance criterion? 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 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~~such policies and procedures for consistency with the established performance criterion.	~~N/A~~

Privacy	Uses and disclosures for specialized government functions – Correctional institutions	~~See above~~§164.512(k)(5) Correctional institutions and other law enforcement custodial situations. (i) Permitted disclosures. 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; or (F) The administration and maintenance of the safety, security, and good order of the correctional institution. (ii) Permitted uses. A covered entity that is a 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) No application after release. 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.	~~Inquire of management as to whether a process is~~How does the covered entity determine whether to disclose PHI to a correctional institution or a law enforcement official with custody of an individual? Are policies and procedures in place to determine ~~if the~~whether a use or disclosure of PHI to a correctional institution or law enforcement official is ~~necessary. Obtain and review PHI disclosed~~permitted? Obtain and review policies and procedures related to disclosures of PHI to correctional institutions or other law enforcement custodial situations for consistency with the established performance criterion. Obtain and review a sample of documentation of disclosures 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	~~N/A~~

			correctional institution. ~~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.~~	
Privacy	Uses and disclosures for specialized government functions – Providing public benefits	(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 data 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 the same or similar populations and the disclosure of protected health information is necessary to coordinate the	Is the covered entity a health plan that is a government program providing public benefits, or is it a government agency administering a government program providing public benefits? If yes. does the covered entity have policies and procedures consistent with the established performance criterion in place to disclose PHI for the purposes listed? Obtain and review the policies and procedures. Obtain and review a sample of such disclosures.	

		covered functions of such programs or to improve administration and management relating to the covered functions of such programs.		
Privacy	Disclosures for workers' compensation	§164.512(~~l)~~ l) Standard: Disclosures for workers' compensation. 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.	~~Inquire of management as to whether a process is in place to determine the need to disclose~~Are policies and procedures in place regarding disclosure of PHI for the purpose of workers' compensation~~. Obtain and review PHI disclosed~~, that are consistent with the established performance criterion? Obtain and review policies and procedures related to disclosures of PHI for workers' compensation or other similar programs for consistency with the established performance criterion. Obtain and review a sample of documentation of disclosures 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~~ 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~~	~~N/A~~

			~~relating to workers' compensation. Whether the disclosure provides~~ or other similar programs, established by law, that provide benefits for work-related injuries~~,~~ or illness~~,~~ without regard to fault.	
Privacy	Requirements for De-Identification of PHI & Re-Identification of PHI	§164.514 (b) Implementation specifications: Requirements for de-identification 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	A covered entity may be , but is not required, to de-identify PHI. Does the covered entity de-identify PHI consistent with the established performance criterion? Obtain and review policies and procedures to determine whether they comply with the established performance criterion. Refer to the de-identification guidance for assistance in these determinations: http://www.hhs.gov/ ocr/privacy /hipaa/ understanding/ coveredentities/ De-identif ication/ guidance.html	

		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 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. §164.514(c) Implementation specifications: Re-identification. 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.		
Privacy	Standard: Minimum Necessary & Minimum Necessary Uses of PHI	(b) ~~§164.514 Other requirements relating to uses and disclosures of~~Standard: Minimum necessary (1) Minimum necessary applies. When using or disclosing protected health information ~~§164.514(d)(2)~~ or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or	~~Inquire of management as to whether access to PHI is restricted. Obtain and review~~Has the covered entity implemented policies and procedures consistent with the requirements of the established performance criterion to identify need for and limit use of PHI? Obtain and review policies and procedures for limiting access to PHI. Elements to consider include, but are not limited to:- -Criteria for determining what level of access a person or class of persons will need -Criteria for modifying, reviewing, or	~~N/A~~

		request. (2) Minimum necessary does not apply. This requirement does not apply to: (i) Disclosures to or requests by a health care provider for treatment; (ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section; (iii) Uses or disclosures made pursuant to an authorization under § 164.508; (iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter; (v) Uses or disclosures that are required by law, as described by § 164.512(a); and (vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter. §164.514(d)(2) Implementation specifications: Minimum necessary uses of protected health information. (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 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.	terminating an individual's access --Efforts to limit access consistent with the needs and conditions described for each person or class of persons -Whether the policies and procedures take into account access to both PHI and ePHI. Obtain and review the access of a sample of workforce members with access to PHI for their corresponding job title and 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.~~ whether the access is consistent with the policies and procedures. 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.	

Privacy	Minimum Necessary - Disclosures of PHI	§164.514 - Other requirements relating to uses and(d)(3) Implementation specification: Minimum necessary 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 (iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure	Inquire of management as to whether Are policies and procedures are in place to limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. ? Obtain and review policies and procedures related to minimum necessary disclosures 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 established performance criterion. Obtain and review a sample of protocols for disclosures made on a routine and recurring basis and determine if such protocols limit to the PHI to what is reasonably necessary to achieve the purpose of the disclosure, as required by 514(d)(3).	N/A

		as the minimum necessary for the stated purpose when: (A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s); (B) The information is requested by another covered entity; (C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or (D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.		
Privacy	Minimum Necessary requests for protected health information	§164.514(d)(4) Implementation specifications: Minimum necessary requests for protected health information. (i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities. (ii) For a request that is made 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 requested to the amount reasonably	Are policies and procedures in place to limit the PHI requested by the entity being audited to the amount minimally necessary to achieve the purpose of the disclosure? Obtain and review policies and procedures related to minimum necessary requests and evaluate the content relative to the specified criteria. Obtain and review a sample of requests made on a routine and recurring basis and determine if they are limited to the PHI reasonably necessary to achieve the purpose of the disclosure, as required by §164.514(d)(4).	

		necessary to accomplish the purpose for which the request is made. (iii) For all other requests, a covered entity must: (A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and (B) Review requests for disclosure on an individual basis in accordance with such criteria.		
Privacy	Minimum Necessary - Other content requirement	§164.514(d)(5) Implementation specification: Other content requirement. 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.	Are policies and procedures in place to address uses, disclosures, or requests for an entire medical record? Obtain and review policies and procedures related to minimum necessary uses, disclosures, or requests for an entire medical record for consistency with the established performance criterion. Obtain and review a sample of use, disclosure, or request for an entire medical record and determine if it is limited to the PHI reasonably necessary to achieve the purpose of the use, disclosure, or request as required by §164.514(d)(5).	
Privacy	Limited Data Sets and Data Use Agreements	§164.514(e)(1) Standard: Limited data set. 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.	Are data use agreements in place between the covered entity and its limited data set recipients, if any? Obtain and review policies and procedures and evaluate the content in relation to the established performance criterion to determine if data use agreements are in place between the covered entity and its limited	

		§164.514(e)(2) Implementation specification: Limited data set: A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images. §164.514(e)(3) Implementation specification: Permitted purposes for uses and disclosures. (i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations. (ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be	data set recipients. Obtain and review a sample data use agreement to determine if the agreements comply with the established performance criterion. Obtain and review a sample limited data set to determine whether it complies with the established performance criterion.	

		used by the covered entity. §164.514(e)(4) Implementation specifications: Data use agreement (i) Agreement required. A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes. (ii) Contents. A data use agreement between the covered entity and the limited data set recipient must: (A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity; (B) Establish who is permitted to use or receive the limited data set; and (C) Provide that the limited data set recipient will: (1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law; (2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement; (3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes		

		aware; (4) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and (5) Not identify the information or contact the individuals. (iii) Compliance. (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.		
Privacy	Uses and Disclosures for Fundraising	§164.514~~ - Other requirements relating to uses~~(f) Fundraising communications. (1) Standard: Uses and disclosures ~~of protected health information §164.514(f) (1) A~~for fundraising. Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation,	~~Inquire of management as to whether~~Is 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.~~ the information set forth in the established performance criterion? Obtain and review policies and procedures	~~N/A~~

		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~~, including name, address, other contact information, age, gender, and date of birth; (ii) Dates of health care provided to an individual~~. (2) (i) The~~; (iii) Department of service information; (iv) Treating physician; (v) Outcome information; and (vi) Health insurance status. (2) Implementation specifications: Fundraising requirements. (i) A 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~~A) is included in the covered entity~~'s notice; (ii) The covered entity must include in any~~'s notice of privacy practices. (ii) With each fundraising ~~materials it sends~~communication made to an individual under this paragraph~~ a description of how~~, a covered entity must provide the individual ~~may opt out of receiving~~with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. ~~(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of~~	and notice of privacy practices and evaluate the content relative to the ~~specified criteria to determine if 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 an example of a disclosure~~established performance criterion. Obtain and review a sample of communications 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~~it contains a clear and conspicuous opportunity to opt-out of further fundraising communications or reference to a mechanism for opting out. Obtain and review documentation that the policies and procedures are ~~updated appropriately and~~ conveyed to the workforce.	

		~~receiving future~~The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost. (iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications. (iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(2)(ii) of this section. (v) A covered entity may provide an individual who has elected not to receive further fundraising communications ~~are not sent~~with a method to opt back in to receive such communications.		
Privacy	Uses and Disclosures for Underwriting and Related Purposes	§164.514~~ Other requirements relating to uses~~(g) Standard: Uses and disclosures ~~of protected health information §164.514(g)~~ for underwriting and related purposes. If a health plan receives protected ~~heath~~health 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~~only use or disclose such protected health information for ~~any other~~such purpose~~, except~~ or as may be	~~Inquire of management as to whether procedures are~~Does the health plan have policies and procedures consistent with the established performance criterion addressing limitations on the use and disclosure of PHI received for underwriting and other purposes? Obtain and review policies and procedures and evaluate the content relative to the established performance criterion. If health insurance or health benefits are not placed with the health plan, do the policies and procedures limit further use or disclosure for such purpose or as may be required by law? See also § 164.502(a)(5)(i) of this document. Are policies and procedures in in place restricting the health plan's uses and/or	~~N/A~~

		required by law, subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic information included in the protected health information. § 164.502(a)(5)(i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan: (A) Except as provided in paragraph (a)(5)(i)(B) of this section: (1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and (4) Other activities related to the creation, renewal, or replacement of a contract of	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~~, subject to the prohibition with respect to genetic information in the PHI ~~limitation for underwriting purposes is included. Obtain and review evidence that the policies and procedures are updated appropriately and conveyed to the workforce.~~ ?	

		health insurance or health benefits. (B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy. From § 160.103 Definitions. Genetic information means: (1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about: (i) The individual's genetic tests; (ii) The genetic tests of family members of the individual; (iii) The manifestation of a disease or disorder in family members of such individual; or (iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. (2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of: (i) A fetus carried by the individual or family member who is a pregnant woman; and (ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology. (3) Genetic information excludes information about the sex or age of any individual. (ii) Genetic services means: (1) A genetic test; (2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) Genetic education. Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or		

		chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.		
Privacy	Verification Requirements	~~§164.514 - Other requirements relating to uses and disclosures of protected health information~~ §164.514(h)(1) Standard: Verification requirements. 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, statement, or representation is a condition of the disclosure under this subpart. ~~(2)~~ (2) Implementation specifications: Verification. (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,	~~Inquire of management as to whether formal or informal~~Are policies and procedures ~~are in place to verify the identity of individuals~~consistent with the established performance criterion in place to verify the identity of persons who request PHI~~.~~? Obtain and review policies and procedures ~~and evaluate the content relative to the specified criteria to determine if a process is in place to verify the identity of~~ regarding verification of the identity of individuals who request PHI. Obtain and review sample documentation, consistent with the established performance criterion, 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~~Such documentation could include a copy of or notation of the official credentials, a completed verification checklist, a copy of the request on official letterhead, etc.	~~N/A~~

		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).		
~~Privacy~~	~~Limited Data Sets and Data Use Agreements~~	~~§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.~~	~~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 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~~	~~N/A~~

			~~that the policies and procedures are updated appropriately and conveyed to the workforce.~~	
~~Privacy~~	~~Limited Data Sets and Data Use Agreements~~	~~§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.~~	~~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.~~	~~N/A~~

~~Privacy~~	~~Re-Identification of PHI~~	~~§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.~~	~~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.~~	~~N/A~~

~~Privacy~~	~~De-Identification of PHI~~	~~§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~~	~~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.~~	~~N/A~~

		~~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.~~		
Privacy	Notice of Privacy Practices Content requirements	~~§164.520 - Notice of Privacy Practices for PHI~~ §164.520(a)(1) Right to notice. Except as provided by	~~Inquire of management as to whether individuals are notified of the potential uses and disclosures of PHI by the~~	~~N/A~~

		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) Required elements. 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 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	~~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. 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~~Does the covered entity have a notice of privacy practices? If yes, verify the current notice contains all the required elements. • Header 164.502(a)(1) – Permitted uses and disclosures Does the covered entity include in its notice a description of the following permitted uses and disclosures? • To the individual • For treatment, payment, or health care operations (with at least one example of a use and disclosure for each purpose) • For public health and safety issues • For research purposes • To comply with the law • To respond to organ and tissue donation requests • To work with a medical examiner or funeral director • To address workers' compensation, law enforcement and other government requests • To respond to lawsuits and legal actions.	

		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 description of the types of uses and disclosures that require an authorization under §164.508(a)(2)– (a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke ~~such~~an 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 informing the individual of such activities, 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~~: (A) In accordance with §164.514(f)(1), the covered entity	Pursuant to an agreement under, or as otherwise permitted by § 164.510 – Uses and disclosures requiring an opportunity to agree or object: (i) For facility direct (ii) For involvement in the individual's care and notification purposes. 64.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required Does the covered entity include in its notice the following uses and disclosures for which an authorization or opportunity to agree or object is not required: • As required by law • For public health activities • Disclosures about victims of abuse, neglect or domestic violence • For health oversight activities • Disclosures for judicial and administrative proceeding • Disclosures for law enforcement purposes • About decedents • For cadaveric organ, eye or tissue donation purposes • For research purposes • To avert a serious threat to health or safety • For specialized government functions. 164.514 (f)(1) – Standard: Uses and disclosures for fundraising. Required Statements: • A statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization • A statement that the individual may revoke an authorization If the covered entity intends to engage in any of the following activities, separate statements for certain uses or disclosures involving fundraising	

		may contact the individual to raise funds for the covered entity~~. (C) A~~ and the individual has a right to opt out of receiving such communications; (B) In accordance with § 164.504(f), the 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; or (C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes. (iv) Individual rights. The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows: (A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under § 164.522(a)(1)(vi); (B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable; (C) The right to inspect and copy protected health information as provided by § 164.524;	o A statement that genetic information cannot be used to decide whether coverage can be given or at what price o A statement that information can be disclosed to a plan sponsor for plan administration. Individual rights: Does 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~~contain a statement of the individual's rights and a description of how the individual may exercise the following rights: • Obtain a copy of the individual's health and claims records • Request that the covered entity correct health and claims records • Request confidential communications • Ask the covered entity to limit what it uses or shares • Obtain a list of those with whom the covered entity has shared information • Obtain a copy of the privacy notice • File a complaint with the entity and the Secretary of HHS CE Duties: Does the covered entity notify individuals of its legal duties with respect to ~~PHI. Verify the privacy notices contain all the required elements specified by the HIPAA Privacy Standard~~their PHI, which are: • To maintain the privacy and security of their PHI • To notify affected individual(s) if a breach occurs that compromised the privacy or	

		(D) The right to amend protected health information as provided by § 164.526; (E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and (F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request. (v) Covered entity's duties. The notice must contain: (A) A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information; (B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and (C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice. (vi) Complaints. The notice must contain	security of their information • To follow the duties and privacy practices described in the notice • The covered entity will not use or share information other than as described here unless authorized in writing. Authorization may be revoked at any time, in writing. Does the notice state that disclosures will be made: • to the Secretary of HHS for HIPAA rules compliance and enforcement purposes Complaints: The notice must contain a statement that the individual has a right to complain to the CE and to the Secretary if they believe their privacy rights have been violated with a brief description of how to file a complaint with the covered entity and a statement of no retaliation for filing a complaint. Contact: The notice must contain the name or title and telephone number of a person or office to contact for further information. Effective date: The notice must contain an effective date.	

		a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint. (vii) Contact. The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii). (viii) Effective date. The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.		
Privacy	Provisions of Notice - Health Plans	§164.520~~ - Notice of Privacy Practices for PHI §164.520(c)(1)~~ (c) Implementation specifications: Provision of notice. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable. (1) Specific requirements for health plans. (i) A health plan must provide the 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~~	~~Specific requirements for health plans: Inquire of management as to how the covered entity the notice to any person upon request.~~ Does the health plan provide its notice of privacy practices consistent with the established performance criterion? Obtain and review the ~~formal or informal~~ policies and procedures in place regarding the provision and posting of the notice of privacy practices.~~ For a selection~~ Has the health plan provided the notice of privacy practices to individuals as required? For a sample 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~~documentation of when and how	~~N/A~~

		~~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. (v) If there is a material change to the notice: (A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan. (B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.	notices were provided. As available, for example, as part of a standard mailing sent to new health plan members, review the notice of privacy practices provided to the selected individuals. Was the notice of privacy practices that was provided to the selected individuals the current notice of privacy practices for the time period in which the notice was provided?	

Privacy	Provisions of Notice - Certain Covered Health Care Providers	~~§164.520 - Notice of Privacy Practices for PHI~~ §164.520(c)(2) Specific requirements for certain covered health care providers. 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	~~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~~Does a covered health care provider with direct treatment relationships with individuals provide its notice of privacy practices consistent with the established performance criterion? Obtain and review the policies and procedures in place regarding the provision of the notice of privacy practices. Obtain and review ~~an example~~a sample of 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~~ Has the covered health care provider provided the notice of privacy practices to individuals as required? From sample of a population 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. Review documentation related to provision of notice to individuals who presented for emergency treatment.	~~N/A~~

		of paragraph (c)(2)(iii) of this section, if applicable.		
Privacy	~~Provisions~~Provision of Notice - Electronic Notice	~~§164.520 - Notice of Privacy Practices for PHI~~ §164.520(c)(3) Specific requirements for electronic notice. (i) A covered entity that maintains a ~~website~~web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the ~~website~~web site and make the notice available electronically through the ~~website.~~ web site. (ii) A covered entity may provide the notice required by this section to an individual by ~~email~~e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the ~~email~~e-mail 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	~~Specific requirements for electronic notice:~~ Does a covered entity that maintains a web site prominently post its notice? Does the covered entity implement policies and procedures, if any, to provide the notice electronically consistent with the standard? Determine whether the entity maintains a web site. If so, observe the web site to determine if the notice of privacy practices is prominently displayed and available. An example of prominent posting of the notice would include a direct link from homepage with a clear description that the link is to the HIPAA Notice of Privacy Practices. If the covered entity provides electronic notice (such as by linkage to a web page or e-mail), obtain and review the policies and procedures regarding the provision of the notice of privacy practices ~~by email~~electronically 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.~~ notice. If the covered entity provides the notice of privacy practices by ~~email~~e-mail or other electronic form, obtain and review ~~an~~	~~N/A~~

		to electronic notice. (iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.	~~example~~the documentation of ~~an~~the agreement with the individual to receive the notice via e-mail or other electronic form. Inquire if covered entity has experienced failures when trying to provide the notice of privacy practices by e-mail. If the covered entity has experienced e-mail transmission failures, obtain and review its attempts to provide a paper copy of the notice via alternative means (e.g., mail).	
Privacy	Joint Notice by Separate Covered Entities	§164.520~~ Notice of Privacy Practices for PHI §164.520(c)(4)~~ (d) Implementation specifications: Joint notice by separate covered entities. 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	~~Covered~~For covered entities that participate in organized health care ~~arrangements: Inquire of management as to whether~~arrangement, does the entity use a joint notice of privacy practices~~ meets the minimum requirements set forth by the HIPAA Privacy Standards.~~ ? If a joint notice is utilized, does the joint notice meet the specific additional criteria for a joint notice? Obtain and review the joint notice of privacy practices to determine whether ~~right to~~ it meets the ~~minimum~~established performance requirements~~ specified by the HIPAA Privacy Standards~~.	~~N/A~~

		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.		
Privacy	Documentation	§164.520(e) Implementation specifications: Documentation. 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.	~~Inquire of management as to whether~~Is the documentation of notice of privacy practices ~~must be~~and the acknowledgement of receipt by individuals of the notice of privacy practices maintained in electronic or written form and retained for a period of ~~six years.~~ 6 years? Obtain and review policies and procedures to assess whether applicable documentation criteria for the notice are established and communicated to appropriate members of the workforce. Obtain and review documentation (copies of all applicable notices and sample of acknowledgements) to determine if (1) the notice of privacy practices~~,~~ ; and (2) (using a	~~N/A~~

			sample) acknowledgements for health care providers with direct ~~patient~~treatment relationships with patients are maintained in electronic or written form and retained for a period of six years.	
Privacy	~~Confidential Communications Requirements~~Right of an Individual to Request Restriction of Uses and Disclosures	§164.522~~ Rights to Request Privacy Protection for PHI §164.522(b)(1)~~ (a)(1) Standard: Right of an individual to request restriction of uses and disclosures. (i) A covered entity must permit ~~individuals to request and must accommodate reasonable requests by individuals to receive communications~~an individual to request that the covered entity restrict: (A) uses or disclosures of protected health 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~~about the individual to carry out treatment, payment, or health care operations; and (B) disclosures permitted under §164.510(b). (ii) Except as provided in paragraph (a)(1)(vi) of this section, 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	~~Inquire of management as to whether~~Does the covered entity ~~permits individuals to request alternative means or alternative locations to receive communications of PHI. Obtain and review formal or informal~~have policies and procedures ~~describing how~~consistent with the established performance criterion to permit an individual ~~may request to receive communications of PHI by alternative means and at alternative locations~~to request that the entity restrict uses or disclosures of PHI for treatment, payment, and health care operations, and disclosures permitted pursuant to §164.510(b)? Obtain and review policies and procedures against the established performance criterion. Has the covered entity agreed to a restriction? If yes, obtain and review sample of documentation of each request and subsequent agreement to determine if restrictions are given effect. Obtain and review all requests since September 23, 2013, for restrictions of information disclosed to a health plan in which the item or service has been paid for out of pocket in full. Obtain and review documentation of covered entity responses to	~~N/A~~

		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. (vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information ~~from~~about the individual to a 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~~if: (A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and (B) The protected health information pertains solely to a health care item or service for which the individual, or person	determine if restrictions are given effect.	

		other than the health plan on behalf of the individual, has paid the covered entity in full.		
Privacy	Terminating a Restriction	§164.522(a)(2) Implementation specifications: Terminating a restriction. 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~~: (A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and (B) Only effective with respect to protected health information created or received after it has so informed the individual.	~~Inquire of management as to whether a process is~~Are policies and procedures in place to terminate restrictions ~~of~~on the use and/or disclosure of PHI~~.~~, consistent with the established performance criterion? Obtain and review policies and procedures ~~around~~related to terminating restrictions of use and/or disclosure of PHI. ~~Obtain~~ Has the covered entity terminated a restriction? If so, obtain and review ~~an example~~a sample 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~~terminations are implemented consistent with the policies and procedures.	~~N/A~~
Privacy	Documentation	§164.522(a)(3) Implementation specification: Documentation. A covered entity ~~that agrees to a restriction~~ must document ~~the~~a restriction in accordance with § 164.530(j) of this subchapter.	~~Inquire of management as to whether~~Does the covered entity, consistent with the established performance criterion, maintain 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	~~N/A~~

			for. Has the covered entity agreed to a restriction in the past 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? If yes, review the documentation required for P64, P65 for consistency with the established performance criterion.	
Privacy	Right of an Individual to Request Restriction of Uses and DisclosuresConfidential Communications Requirements	§164.522 – Rights to Request Privacy Protection for PHI §164.522(a)(1)(i) A covered entity must permit an individual to request that the covered entity restrict: (A) uses or disclosures(b)(1) Standard: Confidential communications requirements. (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications 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	Inquire of management as to whetherDoes the covered entity has a processhave policies and procedures 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 PHIindividuals to request alternative means or alternative locations to receive communications of PHI consistent with the established performance criterion? Does the covered entity have policies and procedures in place to accommodate such requests consistent with the established performance criterion? Obtain and review policies and procedures describing how an individual may request to receive communications of PHI by alternative means and at alternative locations. Obtain and	N/A

		~~may not use or disclose~~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 ~~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~~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. ~~(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~~	review documentation of sample requests and the covered entity response.	

		~~effective under this subpart to prevent uses or disclosures permitted or required under §§164.502(a)(2)(ii), 164.510(a) or 164.512.~~		
Privacy	Right to access	§164.524 ~~–~~(a) Standard: Access ~~of Individuals to PHI §164.524(a)(1)~~ to protected health information. (1) Right of access. 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)~~ , except for (i) psychotherapy notes; and (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. §164.524(b) Implementation specifications: Requests for access and timely action. (1) Individual's request for access. 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~~ §164.524(b) Timely action by the covered	How does the covered entity enable the access rights of an individual? 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.~~ request and obtain access to PHI and to determine whether they comply with the mandated criteria. Determine whether policies and procedures adequately address circumstances in which an access request is made for PHI that is not maintained by the covered entity, per 164.524(d)(3). Obtain and review the notice of privacy practices ~~to identify if~~. Identify whether an individual's right to access in a timely manner is ~~outlined in the notice.~~ correctly described in the notice. Obtain and review access requests which were granted (and documentation of fulfillment, if any) and access requests which were denied. • Verify that access was provided consistent with the policies and procedures • Verify that requests for access were fulfilled in the form and format requested by the	~~N/A~~

		entity. (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows. (A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section. (B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section. (ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)((A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that: (A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; (B) The covered entity may have only one such extension of time for action on a request for access. §164.524(c) Implementation specifications: Provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements. (2) Form of access requested. (i) The	individual if the covered entity can readily produce the PHI in the requested form and format, including electronic format • Determine whether response was made in a timely manner. (e.g., within 30 days of request receipt, unless extension provided consistent with 164.524(b)(2)(ii)) • Determine whether fee charged meets ~~criteria.~~ the reasonable cost based fee requirement of 164.524(c)(4) • If the entity denied access to certain PHI, determine whether it provided access to other PHI requested by the individual that was not excluded, per §164.524(d)(1) • For cases for which access was denied, assess whether the denials, and any reviews made pursuant to individual request, were consistent with the policies and procedures. Inquire of management whether the covered entity has used a standard template or form letter for requesting access to protected health information. If the covered entity has used a standard template or form letter for access, obtain and review the document and determine whether it includes the requirements	

		covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual. (ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. (iii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if: (A) the individual agrees in advance to such a summary or explanation; and (B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation. §164.524(c)(3) Time and manner of access. (i) 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~~(ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information. §164.524(c)(4) Fees. 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~~Labor for copying~~,~~ the protected health information requested by the individual~~; (ii~~, whether in paper or electronic form; (ii) Supplies for creating		

		the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; (iii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and (~~iii~~iv) 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)~~ iii) of this section. §164.524(d) Implementation specifications: Denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements. (1) Making other information accessible. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access. §164.524(d)(3) Other responsibility. If the covered entity does not maintain the protected health 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.		

~~Privacy~~	~~Review of denial of access~~	~~§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~~	~~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.~~	~~N/A~~

		~~action as required by this section to carry out the designated reviewing official's determination.~~		
Privacy	Unreviewable ~~ground~~grounds for denial	§164.524(a)~~(2)~~ Standard: Access to protected health information. (2) Unreviewable grounds for denial. A	~~Inquire of management as to whether the unreviewable denied~~Do policies and procedures exist that dictate the	~~N/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,	circumstances under which denials of 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.~~ ?	

		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 confidentiality and the access requested would be reasonably likely to reveal the source of the information.		
Privacy	Reviewable grounds for denial	§164.524(a)~~(3)~~ Standard: Access to protected health information. (3) Reviewable grounds for denial. 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	~~Inquire of management as to whether the~~Are policies and procedures ~~are~~ in place ~~to have the denial~~regarding review of denials of access ~~reviewed.~~ ? Inquire of management. Obtain and review policies and procedures to determine ~~a~~if the adopted process ~~in place to allow an individual to request a~~for the review of the denial of access complies with the mandated criteria. Review documentation obtained for item 66 for consistency with these requirements	~~N/A~~

		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).~~		
Privacy	Review of denial of access	§164.524(a) Standard: Access to protected health information. (4) Review of a denial of access. 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	Do policies and procedures address request for and fulfilment of review of instances of access denial? Inquire of management. Review policies and procedures to determine whether they comply with the established performance criterion. For example, does the entity have a process for an individual to request and receive a review of a denial of	

		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) Implementation specifications: Denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements: (4) Review of denial requested. 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.	access by a licensed health care professional who did not participate in the original decision to deny the individual's request for access as set forth in §164.524(d)(4)? Does it provide prompt referral of denial for review by licensed health care professional not directly involved in the original denial, determination within a reasonable period of time, and prompt written notice to individual? Review documentation obtained for item 66 for consistency with these requirements	
Privacy	Denial of Access	§164.524(d) Implementation specifications: Denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the	Has the covered entity implemented policies and procedures that ensure that an individual receives a timely, written denial that contains all mandated elements? Inquire of management.	

		following requirements. (1) Making other information accessible. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access. §164.524(d)(2) Denial. 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).	Obtain and review policies and procedures to determine if they comply with the established performance criterion. Obtain and review a sample of denied access requests.	
Privacy	Documentation	§164.524(e) Implementation specification: Documentation. 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	~~Inquire of management as to whether a process of document retention for amendments to PHI is in place.~~ Obtain and review documentation of the current designated record sets subject to access, as well as documentation for the last 6 years (as applicable).	~~N/A~~

		responsible for receiving and processing requests for access by individuals.	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~~access to PHI. Obtain the name or office specified for each year over the preceding 6-year documentation period~~ of six years~~.	
Privacy	Right to Amend	§164.526(a)~~(1)~~ Standard: Right to amend. (1) Right to amend. 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 record set.	~~Inquire of management as to whether a policy exists~~Has the covered entity implemented policies and procedures consistent with the established performance criterion regarding an individual's right to amend their PHI in 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~~? Obtain and review policies and procedures allowing an individual the right to amend protected health information in a designated health record set.	~~N/A~~
Privacy	Denying the Amendment	§164.526(a)~~(2)~~ Standard: Right to amend. (2) Denial of amendment. 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	~~Inquire of management as to whether~~Has the covered entity implemented policies and procedures consistent with the established performance criterion for determining grounds for denying requests~~ for amendment are documented.~~ ?	~~N/A~~

		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.	Obtain and review documentation ~~that outlines a list~~, including policies and procedures, of circumstances by which the entity has grounds for denial of amendment. Verify grounds for denying request for amendment ~~is appropriate~~comply with the established performance criterion.	
Privacy	Accepting the Amendment	§164.526(c) Implementation specifications: Accepting the amendment. If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements. (1) Making the amendment. 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) Informing the individual. 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~~an 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) Informing others. The covered entity must make reasonable efforts to inform	~~Inquire of management as to whether requirements~~Does the covered 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~~have policies and procedures consistent with the established performance criterion for accepting requests for amendments? Review policies and procedures for compliance with amendment criteria. Obtain and review a sample of requests by individuals to amend their PHI or a record about the individual in a designated record set to determine whether they were addressed in accordance with the established performance criterion.	~~N/A~~

		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.		
Privacy	Denying the Amendment	§164.526(d) Implementation specifications: Denying the amendment. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements ~~set forth in the HIPAA Privacy Standards: Provide~~. (1) Denial . The covered entity must provide the individual with a timely, written denial~~. Permit the~~, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain: (i) The basis for the denial, in accordance with paragraph (a)(2) of this section; (ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement; (iii) A statement that, if the individual does not submit a statement of disagreement ~~with instructions on how to submit the statement and inform the individual of complaint procedures (see the HIPAA Privacy Protocol for~~	~~Inquire of management as to whether the requirements the entity must comply with are 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~~Has the covered entity implemented policies and procedures regarding provision of denial consistent with the established performance criterion? Obtain and review entity policies and procedures. Obtain and review a sample of denied requests for consistency with the established performance criterion. Areas of review include timeliness; content of written denial; inclusion of statement of disagreement; provision of rebuttal statements to the individual; recordkeeping;	~~N/A~~

		§164.530). Prepare a written rebuttal if the individual submits statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and (iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established 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). (2) Statement of disagreement. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement. (3) Rebuttal statement. 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	inclusion of denial records when source information is disclosed.	

		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:~~ (5) Future disclosure. (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.		
Privacy	Right to an Accounting of Disclosures of PHI	§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 accordance with §164.514(e); or (ix) That occurred prior to the compliance data for the covered entity. The policies and procedures allow for (2)(i) The covered entity must temporarily suspend an individual's right to requestreceive an accounting of	Inquire of management as to whetherDoes the covered entity have policies and procedures exist forconsistent with the established performance criterion for implementing an individual's right to an accounting of disclosures of PHI. ? Obtain and review policies and procedures in place to determinedocument and respond to a request for an accounting of disclosures is made. Consider whether such documentation limits grounds for denials the ones listed in the established performance criterion.	N/A

		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~~to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede ~~law enforcement or health agency's activities so long as the request is in writing. If the request~~the agency's activities and specifying the time for which such a suspension is required. (ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must ~~document~~: (A) Document the statement, ~~temporarily~~including the identity of the agency or official making the statement; (B) Temporarily suspend the individual's right to ~~the~~an accounting of disclosures ~~and limit~~subject to the statement; and (C) Limit the temporary suspension ~~for~~to no ~~more~~longer than 30 days from the date of the oral statement, unless ~~the~~a written statement ~~is received in writing~~pursuant to paragraph (a)(2)(i) of this section is submitted during that time. (3) An individual may request an accounting of disclosures for a period of time less than six years from the date of		

		the request.		
Privacy	Content of the Accounting	§164.528(b) Implementation specifications: Content of the accounting. The covered entity must provide the individual with a written accounting that meets the following requirements. ~~The content~~ (1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures ~~made~~of protected health information that occurred during the six years ~~prior to the request~~ (or such shorter ~~if~~time period at the request of the individual ~~specifies)~~ as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures ~~made~~ to or by business associates of the covered entity. ~~The content~~ (2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include ~~the date; name and address of the~~for each disclosure: (i) The date of the disclosure; (ii) The name of the entity or person who received the protected health information and, if known, the address of such entity ~~provided the PHI; a~~or person; (iii) A brief description of the ~~PHI~~protected health information disclosed; and ~~a~~(iv) A brief statement of the purpose of the disclosure~~; and why the information was disclosed. If multiple disclosures have been made~~ that reasonably	~~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.~~ Does the covered entity have policies and procedures consistent with the established performance criterion to provide an accounting that contains the content listed? Obtain and review policies and procedures to determine ~~if the covered entity meets the minimum requirements of content for accounting disclosures~~whether the policies and procedures accurately provide for inclusion of the content listed in the established performance criterion. Obtain and review a sample of requests for accounting and entity fulfillment of those requests to consider whether the accountings provided meet the established performance criterion.	~~N/A~~

		informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any. (3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose~~, then the information listed above must be included~~ under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide: (i) The information required by paragraph (b)(2) of this section for the first disclosure ~~along with the~~during the accounting period; (ii) The frequency, periodicity, or number of the disclosures made ~~within~~during the ~~requested~~ accounting period; and ~~the~~(iii) The date of the last such disclosure~~. If~~ during the accounting period. (4)(i) If, during the period covered by the accounting, the covered entity ~~made disclosure for research purposes to~~has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, ~~then the name of the research activity; a~~the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide: (A) The name of the protocol or other research activity; (B) A description,		

		in plain language, of the research protocol or other research activity~~; the type of PHI~~, including the purpose of the research and the criteria for selecting particular records; (C) A brief description of the type of protected health information that was disclosed; ~~the~~(D) The date or period of time ~~the PHI was disclosed along with the last date it was disclosed; the name, address, and phone~~during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period; (E) The name, address, and telephone number of the ~~research sponsor; and a~~entity that sponsored the research and of the researcher to whom the information was disclosed; and (F) A statement that the ~~PHI~~protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity~~ must be included. The covered entity must assist the individual in contacting the research sponsor and researcher~~. (ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.		

Privacy	Provision of the Accounting	§164.528(c) Implementation specifications: Provision of the accounting. -(1) The covered entity must act on the individual[1]'s request for an accounting, no later than 60 days after receipt of such a request, as follows. (i) 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~~covered entity must provide the individual with the accounting requested; or (ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that: (A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and (B) The covered entity	~~Inquire of management as to whether~~Does the covered entity have policies and procedures ~~exist~~consistent with the established performance criterion to provide ~~the~~an individual with ~~the~~a requested accounting of PHI~~.~~ with in the time and fee limitations specified? Obtain and review policies and procedures to determine if ~~a~~the process ~~exists~~ to provide the individual with the requested accounting of PHI complies with the established performance criterion. Review documentation obtained through items P75, P76 for consistency with this criteria.	~~N/A~~

		may have only one such extension of time for action on a request for an accounting. §164.528(c)(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee ~~may be imposed on~~for each subsequent request for an accounting by the same individual ~~with a~~within the 12 month period ~~so long as~~, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.		
Privacy	Documentation	§164.528(d) Implementation specification: Documentation. 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.	~~Inquire~~Does the covered entity document requests for and fulfillment of ~~management as to how~~ accounting of disclosures ~~is documented and retained.~~ consistent with the established performance criterion? 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~~ related to documentation of accountings of disclosures for consistency with the established performance criterion. Review documentation provided for items 75, 76, 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~~	~~N/A~~

			~~determine if the documentation complies with HIPAA Privacy Standards~~established performance criterion.	
Privacy	Personnel designations	(a)(1) Standard: Personnel designations. (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. (ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520. (2) Implementation specification: Personnel designations. A covered entity must document the personnel designations and maintain in written or electronic form for six years.	Has the covered entity designated a privacy official and a contact person consistent with the established performance criterion? Inquire of management (1) who is responsible for the development and implementation of the privacy policies and procedures; and(2) what person or office is designated to receive privacy complaints. Obtain and review documentation to determine if the above items are maintained in electronic or written form and retained for a period of six years.	
Privacy	Training	~~§164.530 - Administrative Requirements~~ §164.530(b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, 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~~ (2) Implementation specifications:	~~Inquire of management as to whether training is provided to~~Does the covered 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~~ train its work force and have a policies and procedures to ensure all members of the workforce receive necessary and appropriate training ~~on HIPAA privacy standards as~~	~~N/A~~

		Training. (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows: (A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity; (B) ~~thereafter~~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~~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 or subpart D of this part, within a reasonable ~~amount of time~~period of time after the material change becomes effective in accordance with paragraph (i) of this section. (ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.	~~mandated by §164.530(b)(1) and §164.530(b)(2)(i). For a selection~~in a timely manner as provided for by the established performance criterion? Obtain and review such policies and procedures. Areas to review include training each new member of the workforce within a reasonable period of time and each member whose functions are affected by a material change in policies or procedures. From the population of new hires within the audit period, obtain and review a sample of documentation ~~showing~~of necessary and appropriate training on the HIPAA ~~privacy compliance~~Privacy Rule that has been provided and completed. Obtain and review documentation that workforce members have been trained on material changes to policies and procedures required by the HITECH Act.	
Breach	Training	§164.530(b) Training. All workforce members must receive training pertaining to the Breach Notification Rule.	164.530(b) - Training Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent with the requirement to provide training pertaining to the Breach Notification Rule. Has the covered entity trained its workforce on the applicable provisions? • Obtain and review the content of covered entity's training materials • Obtain and review evidence that all workforce members received the training,	

			e.g., training sign in sheets.	
Privacy	Safeguards	§164.530(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. (2)(i) Implementation specification: Safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. (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.	Has the covered entity implemented administrative, technical, and physical safeguards to protect all PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart? Does the covered entity reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure? Obtain and review policies and procedures to determine if appropriate administrative, technical, and physical safeguards are in place. Obtain and review documentation of specific safeguards in place from all three categories to reasonably protect the PHI. Such documentation may include, but is not limited to, policies and procedures, photographic or documentary documentation of physical and technical safeguards, and statements from privacy and security officials.	
Breach	Complaints	164.530(d) Complaints. All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rule.	164.530(d) - Complaints to the covered entity Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent with the requirement to provide a process for individuals to complain about the covered entity's compliance with the Breach Notification Rule. Does the covered entity have a process in place for individuals to complain about its	

			compliance with the Breach Notification Rule? Has the covered entity received any such complaints? If yes, obtain and review a list of complaints received in the specified period and the disposition of such complaints, including documentation of actions taken by the covered entity or business associate to investigate and resolve the potential breach. Use sampling methodologies to select complaints to be reviewed and verify that actions taken were consistent with the requirements of the Breach Notification Rule.	
Privacy	Complaints to the Covered Entity	~~§164.530 - Administrative Requirements~~ §164.530(d)(1) Standard: Complaints to the covered entity. 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 requirements of this subpart or subpart D of this part.	~~Inquire of management as to whether formal or informal policies and procedures exist for receiving and processing complaints over the entity's privacy practices. Obtain and review formal or informal~~Does the covered entity have a process for individuals to make complaints, consistent with the requirements of the established performance criterion? Obtain and review 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.~~	~~N/A~~
Privacy	Complaints to the Covered Entity	§164.530(d)(2) Implementation specification: Documentation of complaints. As required by paragraph (j) of this section, a covered entity must	Has the covered entity documented all complaints received and their disposition consistent with the performance criteria?	

		document all complaints received, and their disposition, if any.	Obtain and review a sample of documentation of complaints for consistency with the established performance criterion.	
Breach	Sanctions	164.530(e) Sanctions. All covered entities must sanction workforce members for failing to comply with the Breach Notification Rule.	164.530(e) – Sanctions Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent with the requirement to sanction a covered entity's workforce members. Has the covered entity sanctioned any workforce members for failing to comply with its policies and procedures as they relate to the Breach Notification Rule? If yes, obtain and review a complete list of sanctions, including the type of sanction applied and the type of action that led to the sanction and any other relevant information. Use sampling methodologies to select sanctions to be reviewed and verify that actions taken were consistent with the requirements of the Breach Notification Rule.	
Privacy	Sanctions	~~§164.530 - Administrative Requirements~~ §164.530(e)(1) Standard: Sanctions. 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 or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.	~~Inquire of management as to whether~~Does the covered entity apply appropriate sanctions ~~are in place~~ against members of the ~~covered entity's~~ workforce who fail to comply with the privacy policies and procedures~~.~~ of the entity or the Privacy Rule? 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~~	~~N/A~~

		(2) Implementation specification: Documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.	~~practices. From a population of instances of individual/employee non-compliance within the audit period, obtain~~the entity has and applies sanctions consistent with the established performance criterion. Obtain and review documentation of the application of sanctions to a sample of workforce members to determine whether appropriate sanctions were applied. ~~Obtain and review evidence that the policies and procedures are updated and conveyed to the workforce~~(Note: OCR is not looking for violations in order to take enforcement action; we are restricting our analysis to whether appropriate sanctions consistent with the entity policies have been applied.)	
~~Privacy~~	~~Policies and Procedures~~	~~§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.~~	~~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.~~	~~N/A~~

~~Privacy~~	~~Administrative, Technical and Physical Safeguards~~	~~§164.530 - Administrative Requirements §164.530(c)(2)(i) A covered entity must reasonably safeguard protected health 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.~~	~~Inquire of management as to whether administrative, 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.~~	~~N/A~~
Privacy	Mitigation	~~§164.530 - Administrative Requirements~~ §164.530(f)~~(1)~~ Standard: Mitigation. 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.	~~Inquire of management as to whether~~Does the covered entity ~~mitigates~~mitigate 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~~for consistency with the established performance criterion. Determine whether a process is in place to ~~help~~	~~N/A~~

			~~management~~ ensure ~~corrective action/~~mitigation ~~plans~~actions are ~~developed~~taken pursuant to ~~relevant~~the policies ~~or~~and procedures. From a population of instances of non-compliance within the audit 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~~the policies and procedures. [Note: OCR is not looking for violations in order to take enforcement action; we are restricting our analysis to whether appropriate mitigation plans consistent with the entity policies have been developed and applied] Obtain and review documentation that the policies and procedures are ~~updated appropriately and~~ conveyed to the workforce.	
Privacy	Refraining from Intimidating or Retaliatory Acts	~~§164.530 - Administrative Requirements~~ §164.530(g) Standard: Refraining from intimidating or retaliatory acts. A covered entity— (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;	~~Inquire of management as to whether~~Has the covered entity implemented policies and procedures ~~exist preventing~~addressing the prevention of 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~~	~~N/A~~

		and (2) must refrain from intimidation and retaliation as provided in §160.316.	~~to the specified criteria~~ to determine if anti-intimidation and anti-retaliatory standards exist. Obtain and review ~~evidence~~documentation that the policies and procedures are ~~updated appropriately and~~ conveyed to the workforce.	
Breach	Refraining from Retaliatory Acts	164.530(g) Refraining from Retaliatory Acts. All covered entities must have policies and procedures in place to prohibit retaliatory acts.	164.530(g) – Refraining from Retaliatory Acts Does the covered entity have appropriate policies and procedures in place to prohibit retaliation against any individual for exercising a right or participating in a process (e.g., assisting in an investigation by HHS or other appropriate authority or for filing a complaint) or for opposing an act or practice that the person believes in good faith violates the Breach Notification Rule? Obtain and review such policies and procedures.	
Privacy	Waiver of rights	§164.530(h) Standard: Waiver of rights. A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.	Has the covered entity required individuals to waive their right to complain to the Secretary of HHS about a covered entity or business associate not complying with these Rules, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits? Obtain and review policies and procedures and patient/health plan member intake information to ensure that waiver is not required.	
Breach	Waiver of Rights	164.530(h) Waiver of Rights.	164.530(h) – Waiver of Rights Does the covered entity have appropriate	

		All covered entities must have policies and procedures in place to prohibit it from requiring an individual to waive any rights under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.	policies and procedures in place to prohibit it from requiring an individual to waive any right under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits? Obtain and review such policies and procedures. If patient or health plan member intake forms are used, obtain and review to confirm that such a requirement is not contained within them.	
Privacy	Policies and Procedures	§164.530(i)(1) Standard: Policies and procedures. 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 and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart. (2) Standard: Changes to policies and procedures. (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 or subpart D of this part. (ii) When a covered entity changes a privacy practice that is stated in the notice	Has the covered entity implemented policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, and other requirements of the HIPAA Privacy Rule? Obtain and review documentation that, consistent with the established performance criterion address the following: - The policies and procedures are reasonably designed to ensure compliance for the size and type of activities performed. - The entity changes these policies and procedures as necessary to comply with changes in the law. - The entity documents and implements such changes promptly. - Any corresponding material changes are made to the notice of privacy practices. Obtain copies of policies and procedures in place in the previous calendar year and January 1, 2012, and the corresponding notices of privacy practices in effect on those dates. Determine whether material changes (e.g., for health plans, limits on use of genetic information for underwriting purposes; for health care providers, that a request for	

		described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or (iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section. (3) Implementation specification: Changes in law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law. (4) Implementation specifications: Changes to privacy practices stated in the notice. (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must: (A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice,	restriction must be accepted in certain situations) required by the HITECH omnibus rule are incorporated into the recent policies and procedures and are reflected in the notice of privacy practices.	

		complies with the standards, requirements, and implementation specifications of this subpart; (B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and (C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice. (ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that: (A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and (B) Such change is effective only with respect to protected health information created or received after the effective date of the notice. (5) Implementation specification: Changes to other policies or procedures. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that: (i) The policy or procedure, as revised,		

		complies with the standards, requirements, and implementation specifications of this subpart; and (ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.		
Breach	Policies and Procedures	164.530(i) Policies and Procedures. All covered entities must have policies and procedures that are consistent with the requirements of the Breach Notification Rule.	164.530(i) – Policies and Procedures Does the covered entity have policies and procedures that are consistent with the requirements of the Breach Notification Rule? • Obtain and review the covered entity's policies and procedure for evaluating the appropriate action under the Breach Notification Rule when there is an impermissible use or disclosure of PHI. • Obtain and review the covered entity's policies and procedures for providing notifications to individuals, the media (if applicable), and the Secretary. • Obtain and review the covered entity's policies and procedures for requiring business associates to report an impermissible use or disclosure of PHI to the covered entity and the covered entity's process for handling such reports.	
Privacy	Documentation	§164.530(j)(1) Standard: Documentation. A covered entity must: (i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form; (ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and (iii) If an action, activity, or designation is required	Does the entity maintain all required policies and procedures, written communication, and documentation in written or electronic form? Are such documentations retained for the required time period?	

		by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation. (iv) Maintain documentation sufficient to meet its burden of proof under § 164.414(b). (2) Implementation specification: Retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.		
Breach	Documentation	164.530(j) Documentation. All covered entities must have policies and procedures in place for maintaining documentation.	164.530(j) - Documentation Does the covered entity have policies and procedures for maintaining documentation consistent with the requirements at §164.530(j)? • Obtain and review documentation that the covered entity maintains its policies and procedures, in written or electronic form, until 6 years after the later of the date of their creation or the last effective date. • Obtain and review documentation that the covered entity maintains all other documentation required by 164.530(j)(1) until 6 years after the later of the date of their creation or the last effective date.	
Security	Business Associate Contracts or Other Arrangements	§ 164.314(a)(1): The contract or other arrangement between the covered entity and its business associate required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.	Does the entity have policies and procedures in place regarding its contractual arrangements with contractors or other entities to which it discloses ePHI for use on its behalf? Elements to review may include but are not limited to:	Required

			• Does the entity use a standard business associate contract with contractors or other entities to which it discloses ePHI • What is the approval process for deviations of standard business associate contracts Obtain and review the entity's standard business associate contract template(s). Evaluate and determine that the entity's standard business associate contract template(s) meet the requirements of 45 CFR § 164.314(a)(2)(i), § 164.314(a)(2)(ii), or § 164.314(a)(2)(iii), as applicable. Obtain and review documentation demonstrating the entity's approval process when deviations affecting the implementation of safeguards to protect ePHI are considered. Evaluate and determine if the entity's policies for approving deviations affecting safeguards to protect ePHI are appropriate.	
Security	Business associate contracts	§ 164.314(a)(2)(i)(A): The contract must provide that the business associate will—(A) Comply with the applicable requirements of this subpart;	Does the entity have policies and procedures in place regarding the content of its business associate contracts to ensure that its business associates will comply with applicable requirements of Subpart C of 45 CFR Part 164? Obtain and review business associate contracts. Evaluate and determine if the business associate contracts provide that the entity's business associates shall implement appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to ePHI to prevent the use or disclosure of PHI other than as provided for by the business associate contract.	Required

Security	Business associate contracts.	§ 164.314(a)(2)(i)(B):The contract must provide that the business associate will, in accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section	Does the entity have policies and procedures in place requiring that its business associate contracts or other arrangements require that subcontractors that create, receive, maintain or transmit ePHI on behalf of its business associates agree to comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a)? Obtain and review business associate contracts. Evaluate and determine if the business associate contracts require that business associate's subcontractors comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a).	Required
Security	Business associate contracts.	§ 164.314(a)(2)(i)(C): The contract must provide that the business associate will report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410	Does the entity have policies and procedures in place regarding the content of its business associate contracts to ensure that its business associates will report any security incident of which it becomes aware, including breaches of unsecured PHI, as required by 45 CFR § 164.410? Obtain and review business associate contracts. Evaluate and determine if the business associate contracts require that business associates report any security incident of which it becomes aware, including breaches of unsecured PHI, as required by 45 CFR § 164.410. Obtain and review documentation demonstrating that the entity's business	Required

			associates have reported security incidents of which it was aware, including breaches of unsecured PHI, as required by 45 CFR § 164.410.	
Security	Other Arrangements	§ 164.314(a)(2)(ii): The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).	Does the entity have policies and procedures in place regarding other arrangements to have in place (e.g., a Memorandum of Understanding if the covered entity and business associate are government agencies) that meet the requirements of 45 CFR § 164.504(e)(3)? Obtain and review documentation of the entity's other arrangements with business associates. Evaluate and determine if the other arrangements meet the requirements of 45 CFR § 164.504(e)(3).	Required
Security	Business associate contracts with subcontractors	§ 164.314(a)(2)(iii): The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	Does the business associate have policies and procedures in place regarding business associate contracts or other arrangements with its subcontractors such that the requirements of 45 CFR § 164.314(a)(2)(i)-(ii) would apply to the business associate and its subcontractors in the same manner as such requirements apply to a covered entity and its business associates? Obtain and review business associate contracts entered into with subcontractors. Evaluate and determine if the business associate contracts require that the requirements of 45 CFR § 164.314(a)(2)(i)-(ii) would apply to the business associate and its subcontractor in the same manner as such requirements apply to a	Required

			covered entity and its business associates.	
Security	Requirements for Group Health Plans	§ 164.314(a)(b)(1): Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Does the group health plan have policies and procedures in place to ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan? Obtain and review plan documents. Evaluate and determine that, except when the only ePHI disclosed to a plan sponsor is in accordance with 45 CFR § 164.504(f)(1)(ii) or (iii) or authorized under 45 CFR § 164.508, that the plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan.	Required
Security	Group Heath Plan Implementation Specification	§ 164.314(b)(2)(i): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.	Do the plan documents of the group health plan include language that requires the sponsor to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan? Obtain and review plan documentation. Evaluate and determine that the plan documents of the group health plan requires the sponsor to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of	Required

			the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan.	
Security	Group Heath Plan Implementation Specification	§ 164.314(b)(2)(ii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.	Do the plan documents of the group health plan incorporate provisions to ensure that adequate separation required by 45 CFR § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures? Obtain and review plan documentation. Evaluate and determine that the plan documents of the group health plan ensures adequate separation between the group health plan and the plan sponsor, including the sponsor's employees, classes of employees, or other persons who will be given access to the ePHI.	Required
Security	Group Heath Plan Implementation Specification	§ 164.314(b)(2)(iii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.	Do the plan documents of the group health plan incorporate provisions to include language that requires the sponsors to ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information? Obtain and review plan documentation. Evaluate and determine that the plan documents of the group health plan requires that plan sponsors ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.	Required
Security	Group Heath Plan Implementation Specification	§ 164.314(b)(2)(iv): The plan documents of the group health plan must be amended to incorporate provisions to require the	Do the plan documents of the group health plan incorporate provisions to include language that requires plan sponsors to report	Required

		plan sponsor to-- (iv) Report to the group health plan any security incident of which it becomes aware.	to the group health plan any security incident of which it becomes aware? Obtain and review plan documentation. Evaluate and determine that the plan documents of the group health plan requires that plan sponsors report to the group health plan any security incident, including any breach of unsecured ePHI, of which it becomes aware.	