HIPAA Security Standards Assessment

Administrative Safeguards

Security Management Process (§ 164.308(a)(1)) HIPAA Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Identify Relevant Information Systems	• Identify all information systems that house EPHI. • Include all hardware and software that are used to collect, store, process, or transmit EPHI. • Analyze business functions and verify ownership and control of information system elements as necessary.	• Are all hardware and software for which [Organization's name] is responsible periodically inventoried? • Have hardware and software that maintains or transmits EPHI been identified? • Does this inventory include removable media and remote access devices? • Is the current information system configuration documented, including connections to other systems?		
2. Conduct Risk Assessment	• Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by [Organization's name].	• Are there any prior risk assessments, audit comments, security requirements, and/or security test results? • Is there risk alerts available from other agencies (DIR) and/or vendors? • Is there a current and tested disaster recovery plan in place? • Has responsibility been assigned to check all hardware and software, including hardware and software used for remote access, to determine whether selected security settings are enabled? • Is there an analysis of current safeguards and their effectiveness relative to the identified risks? • Have all processes involving EPHI been considered, including creating, receiving, maintaining, and transmitting it?		
3. Implement a Risk Management Program	• Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.	• Do current safeguards ensure the confidentiality, integrity, and availability of all EPHI? • Do current safeguards protect against reasonably anticipated uses or disclosures of EPHI? • Has [Organization's name] protected against all reasonably anticipated threats or hazards to the security and integrity of EPHI? • Has [Organization's name] assured compliance with all policies and procedures by its workforce?		
4. Acquire IT Systems and Services	• 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 solution to the intended environment; The sensitivity of the data; [Organization's name]'s security policies, procedures, and standards; and Other requirements such as resources available for operation, maintenance, and training.	• Will new security controls work with the existing IT architecture? • Have the security requirements of [Organization's name] been compared with the security features of existing or proposed hardware and software? • Has a cost-benefit analysis been conducted to determine the reasonableness of the investment given the security risks identified?		
5. Create and Deploy Policies and Procedures	• Implement the decisions concerning the management, operational, and technical controls selected to mitigate identified risks. • Create policies that clearly establish roles and responsibilities and assign ultimate responsibility for the implementation of each control to particular individuals or offices. • Create procedures to be followed to accomplish particular security-related tasks.	• Are policies and procedures in place for security? • Is there a formal contingency plan? • Is there a process for communicating policies and procedures to the affected employees? • Are policies and procedures reviewed and updated as needed?		
6. Develop and Implement a Sanction Policy	• Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of [Organization's name]. • Develop policies and procedures for imposing appropriate sanctions (e.g., reprimand, termination) for noncompliance with [Organization's name]'s security policies. • Implement sanction policy as cases arise.	• Is there a formal process in place to address system misuse, abuse, and fraudulent activity? • Have employees been made aware of policies concerning sanctions for inappropriate access, use, and disclosure of EPHI? • Has the need and appropriateness of a tiered structure of sanctions that accounts for the magnitude of harm and possible types of inappropriate disclosures been considered? • How will managers and employees be notified regarding suspect activity?		
7. Develop and Deploy the Information System Activity Review Process	• Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	• Who is responsible for the overall process and results? • How often will reviews take place? • How often will review results be analyzed? • Where will audit information reside (e.g., separate server)?		
8. Develop Appropriate Standard Operating Procedures	• Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports.	• How will exception reports or logs be reviewed? • Where will monitoring reports be filed and maintained?		
9. Implement the Information System Activity Review and Audit Process	• Activate the necessary review process. • Begin auditing and logging activity.	• What mechanisms will be implemented to assess the effectiveness of the review process (measures)? • What is the plan to revise the review process when needed?		
Assigned Security Responsibility (§ 164.308(a)(2)) **HIPAA Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**

1. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	• Select a Security Official To Be Assigned Responsibility for HIPAA Security	• Identify the individual who has final responsibility for security. • Select an individual who is able to assess effective security and to serve as the point of contact for security policy, implementation, and monitoring. • Who in [Organization's name]— Oversees the development and communication of security policies and procedures? Is responsible for conducting the risk assessment? Handles the results of periodic security evaluations and continuous monitoring? Directs IT security purchasing and investment? Ensures that security concerns have been addressed in system implementation		
2. Assign and Document the Individual's Responsibility	• Document the assignment to one individual's responsibilities in a job description • Communicate this assigned role to the entire organization.	• Is there a complete job description that accurately reflects assigned security duties and responsibilities? • Have the staff members in [Organization's name] been notified as to whom to call in the event of a security problem?		

Workforce Security (§ 164.308(a)(3))

HIPAA Standard: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. In other words, the clearance process must establish the procedures to verify that a workforce member does in fact have the appropriate access for their job function.

Key Activities	Descriptions	Questions to Answer	How is the Standard Implemented?	Departmental Implementation
1. Implement Procedures for Authorization and/or Supervision	• Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.	• Have chains of command and lines of authority been established? • Have staff members been made aware of the identity and roles of their supervisors?		
2. Establish Clear Job Descriptions and Responsibilities	• Define roles and responsibilities for all job functions. • Assign appropriate levels of security oversight, training, and access.	• Identify in writing who has the business need—and who has been granted permission—to view, alter, retrieve, and store EPHI, and at what times, under what circumstances, and for what purposes. • Are there written job descriptions that are correlated with appropriate levels of access? • Have staff members been provided copies of their job descriptions, informed of the access granted to them, as well as the conditions by which this access can be used?		
3. Establish Criteria and Procedures for Hiring and Assigning Tasks	• Ensure that staff members have the necessary knowledge, skills, and abilities to fulfill particular roles, e.g., positions involving access to and use of sensitive information. • Ensure that these requirements are included as part of the personnel hiring process.	• Have the qualifications of candidates for specific positions been checked against the job description? • Have determinations been made that candidates for specific positions are able to perform the tasks of those positions?		
4. Establish a Workforce Clearance Procedure	• Implement procedures to determine that the access of a workforce member to EPHI is appropriate. • Implement appropriate screening of persons who will have access to EPHI. • Implement a procedure for obtaining clearance from appropriate offices or individuals where access is provided or terminated.	• Is there an implementation strategy that supports the designated access authorities? • Are applicants' employment and educational references checked, if reasonable and appropriate? • Have background checks been completed, if reasonable and appropriate? • Do procedures exist for obtaining appropriate sign-offs to grant or terminate access to EPHI?		
5. Establish Termination Procedures	• Implement procedures for terminating access to EPHI when the employment of a workforce member ends or as required by determinations made as specified in §164.308(a)(3)(ii)(B). • Develop a standard set of procedures that should be followed to recover access control devices ([Organization's name] IDs, keys, access cards, etc.) when employment ends. • Deactivate computer access accounts (e.g., disable user IDs and passwords). See the Access Controls Standard.	• Are there separate procedures for voluntary termination (retirement, promotion, transfer, change of employment) vs. involuntary termination (termination for cause reduction in force, involuntary transfer, and criminal or disciplinary actions), if reasonable and appropriate? • Is there a standard checklist for all action items that should be completed when an employee leaves (return of all access devices, deactivation of logon accounts [including remote access], and delivery of any needed data solely under the employee's control)?		

Information Access Management (§ 164.308(a)(4))

HIPAA Standard: 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.

Key Activities	Descriptions	Questions to Answer	How is the Standard Implemented?	Departmental Implementation
1. Isolate Healthcare Clearinghouse Functions	• If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the larger organization. • Determine if a component of [Organization's name] constitutes a healthcare clearinghouse under the HIPAA Security Rule. • If no clearinghouse functions exist, document this finding. • If a clearinghouse exists within [Organization's name], implement procedures for access consistent with the HIPAA Privacy Rule. • In other words, the clearance process must establish the procedures to verify that a workforce member does in fact have the appropriate access for their job function.	• Does the healthcare clearinghouse share hardware or software with a larger organization of which it is a part? • Does the healthcare clearinghouse share staff or physical space with staff from a larger organization? • Has a separate network or subsystem been established for the healthcare clearinghouse, if reasonable and appropriate? •Has staff of the healthcare clearinghouse been trained to safeguard EPHI from disclosure to the larger organization, if required for compliance with the HIPAA Privacy Rule?		

2. Implement Policies and Procedures for Authorizing Access	• Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism. • Decide how access will be granted to workforce members within [Organization's name]. • Select the basis for restricting access. • Select an access control method (e.g., identity-based, role-based, or other reasonable and appropriate means of access.) • Determine if direct access to EPHI will ever be appropriate for individuals external to [Organization's name] (e.g., business partners or patients seeking access to their own EPHI).	• Do [Organization's name]'s IT systems have the capacity to set access controls? • Are there documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties? • Does [Organization's name] grant remote access to EPHI? • What method(s) of access control is (are) used (e.g., identity-based, role-based, location-based, or a combination)?		
3. Implement Policies and Procedures for Access Establishment and Modification	• Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. •Establish standards for granting access. •Provide formal authorization from the appropriate authority before granting access to sensitive information.	• Are duties separated such that only the minimum necessary EPHI is made available to each staff member based on their job requirements		
4. Evaluate Existing Security Measures Related to Access Controls	• Evaluate the security features of access controls already in place, or those of any planned for implementation, as appropriate. • Determine if these security features involve alignment with other existing management, operational, and technical controls, such as policy standards and personnel procedures, maintenance and review of audit trails, identification and authentication of users, and physical access controls.	• Are there policies and procedures related to the security of access controls? If so, are they updated regularly? • Are authentication mechanisms used to verify the identity of those accessing systems protected from inappropriate manipulation? • Does management regularly review the list of access authorizations, including remote access authorizations, to verify that the list is accurate and has not been inappropriately altered?		

Security Awareness and Training (§ 164.308(a)(5))
HIPAA Standard: Implement a security awareness and training program for all members of its workforce (including management).

Key Activities	Descriptions	Questions to Answer	How is the Standard Implemented?	Departmental Implementation
1. Conduct a Training Needs Assessment	• Determine the training needs of [Organization's name]. • Interview and involve key personnel in assessing security training needs.	• What awareness, training, and education programs are needed? •What is the current status regarding how these needs are being addressed (e.g., how well are current efforts working)? • Where are the gaps between the needs and what is being done (e.g., what more needs to be done)? • What are the training priorities in terms of content and audience?		
2. Develop and Approve a Training Strategy and a Plan	• Address the specific HIPAA policies that require security awareness and training in the security awareness and training program. • Outline in the security awareness and training program the scope of the awareness and training program; the goals; the target audiences; the learning objectives; the deployment methods, evaluation, and measurement techniques; and the frequency of training.	• Is there a procedure in place to ensure that everyone in [Organization's name] receives security awareness training? • What type of security training is needed to address specific technical topics based on job responsibility? • When should training be scheduled to ensure that compliance deadlines are met? • Has [Organization's name] considered the training needs of non-employees (e.g., contractors, interns)?		
3. Protection from Malicious Software; Log-in Monitoring; and Password Management	•As reasonable and appropriate, train employees regarding procedures for: o Guarding against, detecting, and reporting malicious software; o Monitoring log-in attempts and reporting discrepancies; and o Creating changing, and safeguarding passwords. • Incorporate information concerning staff members' roles and responsibilities in implementing these implementation specifications into training and awareness efforts.	• Do employees know the importance of timely application of system patches to protect against malicious software and exploitation of vulnerabilities? • Are employees aware that log-in attempts may be monitored? • Do employees that monitor log-in attempts know to whom to report discrepancies? • Do employees understand their roles and responsibilities in selecting a password of appropriate strength, changing the password periodically (if required), and safeguarding their password?		
4. Develop Appropriate Awareness and Training Content, Materials, and Methods	• Select topics that may need to be included in the training materials. • Incorporate new information from email advisories, online IT security daily news Web sites, and periodicals, as is reasonable and appropriate. • Consider using a variety of media and avenues according to what is appropriate for [Organization's name] based on workforce size, location, level of education, etc.	• Have employees received a copy of, and do they have ready access to, [Organization's name]'s security procedures and policies? • Do employees know whom to contact and how to handle a security incident? • Do employees understand the consequences of noncompliance with the stated security policies? • Do employees who travel know how to handle physical laptop security issues and information security issues? • Has [Organization's name] researched available training resources? • Is dedicated training staff available for delivery of security training? If not, who will deliver the training?		
5. Implement the Training	• Schedule and conduct the training outlined in the strategy and plan. • Implement any reasonable technique to disseminate the security messages in an organization, including newsletters, screensavers, videotapes, email messages, teleconferencing sessions, staff meetings, and computer-based training.	• Have all employees received adequate training to fulfill their security responsibilities? • Are there sanctions if employees do not complete required training?		
6. Implement Security Reminders	• Implement periodic security updates. • Provide periodic security updates to staff, business associates, and contractors.	• What methods are available or already in use to make or keep employees aware of security, e.g., posters or booklets? • Is security refresher training performed on a periodic basis (e.g., annually)? • Is security awareness discussed with all new hires? • Are security topics reinforced during routine staff meetings?		

7.Monitor and Evaluate Training Plan	• Keep the security awareness and training program current. • Conduct training whenever changes occur in the technology and practices as appropriate. • Monitor the training program implementation to ensure that all employees participate. • Implement corrective actions when problems arise.	• Are employee training and professional development programs documented and monitored, if reasonable and appropriate? • How are new employees trained on security? • Are new non-employees (e.g., contractors, interns) trained on security?		
Security Incident Procedures (§ 164.308(a)(6)) **HIPAA Standard: Implement policies and procedures to address security incidents.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Determine Goals of Incident Response	• Gain an understanding as to what constitutes a true security incident. Under the HIPAA Security Rule, a security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 CFR § 164.304) • Determine how [Organization's name] will respond to a security incident. • Establish a reporting mechanism and a process to coordinate responses to the security incident. • Provide direct technical assistance, advise vendors to address product-related problems, and provide liaisons to legal and criminal investigative groups as needed.	• Has the HIPAA-required security risk assessment resulted in a list of potential physical or technological events that could result in a breach of security? • Is there a procedure in place for reporting and handling incidents? • Has an analysis been conducted that relates reasonably anticipated threats and hazards to [Organization's name] that could result in a security incident to the methods that would be used for mitigation? • Have the key functions of [Organization's name] been prioritized to determine what would need to be restored first in the event of a disruption?		
2. Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism	• Determine if the size, scope, mission, and other aspects of [Organization's name] justify the reasonableness and appropriateness of maintaining a standing incident response team. • Identify appropriate individuals to be a part of a formal incident response team, if [Organization's name] has determined that implementing an incident response team is reasonable and appropriate.	• Do members of the team have adequate knowledge of [Organization's name]'s hardware and software? • Do members of the team have the authority to speak for [Organization's name] to the media, law enforcement, and clients or business partners? • Has the incident response team received appropriate training in incident response activities?		
3. Develop and Implement Procedures to Respond to and Report Security Incidents	• Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to [Organization's name]; and document security incidents and their outcomes. • Document incident response procedures that can provide a single point of reference to guide the day-to-day operations of the incident response team. • Review incident response procedures with staff with roles and responsibilities related to incident response, solicit suggestions for improvements, and make changes to reflect input if reasonable and appropriate. • Update the procedures as required based on changing organizational needs.	• Has [Organization's name] determined that maintaining a staffed security incident hotline would be reasonable and appropriate? • Has [Organization's name] determined reasonable and appropriate mitigation options for security incidents? • Has [Organization's name] determined that standard incident report templates to ensure that all necessary information related to the incident is documented and investigated are reasonable and appropriate? • Has [Organization's name] determined under what conditions information related to a security breach will be disclosed to the media? • Have appropriate (internal and external) persons who should be informed of a security breach been identified and a contact information list prepared? • Has a written incident response plan been developed and provided to the incident response team?		
4. Incorporate Post-Incident Analysis into Updates and Revisions	• Measure effectiveness and update security incident response procedures to reflect lessons learned, and identify actions to take that will improve security controls after a security incident.	• Does the incident response team keep adequate documentation of security incidents and their outcomes, which may include what weaknesses were exploited and how access to information was gained? • Do records reflect new contacts and resources identified for responding to an incident? • Does [Organization's name] consider whether current procedures were adequate for responding to a particular security incident?		
Contingency Plan (§ 164.308(a)(7)) **HIPAA Standard: 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.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Develop Contingency Planning Policy	• Define [Organization's name]'s overall contingency objectives. • Establish [Organization's name]'s framework, roles, and responsibilities for this area. • Address scope, resource requirements, training, testing, plan maintenance, and backup requirements.	• What critical services must be provided within specified timeframes? o Patient treatment, for example, may need to be performed without disruption. o By contrast, claims processing may be delayed during an emergency with no long-term damage to [Organization's name]. • Have cross-functional dependencies been identified so as to determine how the failure in one system may negatively impact another one?		
2. Conduct an Applications and Data Criticality Analysis	• Assess the relative criticality of specific applications and data in support of other Contingency Plan components. • Identify the activities and material involving EPHI that are critical to business operations. • Identify the critical services or operations, and the manual and automated processes that support them, involving EPHI. • Determine the amount of time [Organization's name] can tolerate disruptions to these operations, material, or services (e.g., due to power outages). • Establish cost-effective strategies for recovering these critical services or	• What hardware, software, and personnel are critical to daily operations? • What is the impact on desired service levels if these critical assets are not available? • What, if any, support is provided by external providers (Internet service providers [ISPs], utilities, or contractors)? • What is the nature and degree of impact on the operation if any of the critical resources are not available?		

3. Identify Preventive Measures	• Identify preventive measures for each defined scenario that could result in loss of a critical service operation involving the use of EPHI. • Ensure that identified preventive measures are practical and feasible in terms of their applicability in a given environment.	• What alternatives for continuing operations of [Organization's name] are available in case of loss of any critical function/resource? • What is the cost associated with the preventive measures that may be considered? • Are the preventive measures feasible (affordable and practical for the environment)? • What plans, procedures, or agreements need to be initiated to enable implementation of the preventive measures, if they are necessary?		
4. Develop Recovery Strategy	• Finalize the set of contingency procedures that should be invoked for all identified impacts, including emergency mode operation. The strategy must be adaptable to the existing operating environment and address allowable outage times and associated priorities identified in step 2. • Ensure, if part of the strategy depends on external organizations for support, that formal agreements are in place with specific requirements stated.	• Have procedures related to recovery from emergency or disastrous events been documented? • Has a coordinator who manages, maintains, and updates the plan been designated? • Has an emergency call list been distributed to all employees? Have recovery procedures been documented? • Has a determination been made regarding when the plan needs to be activated (anticipated duration of outage, tolerances for outage or loss of capability, impact on service delivery, etc.)?		
5. Data Backup Plan and Disaster Recovery Plan	• Establish and implement procedures to create and maintain retrievable exact copies of EPHI. • Establish (and implement as needed) procedures to restore any loss of data.	• Is there a formal, written contingency plan? • Does it address disaster recovery and data backup? • Do data backup procedures exist? • Are responsibilities assigned to conduct backup activities? • Are data backup procedures documented and available to other staff?		
6. Develop and Implement an Emergency Mode Operation Plan	• Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode. • "Emergency mode" operation involves only those critical business processes that must occur to protect the security of EPHI during and immediately after a crisis situation.	• Have procedures been developed to continue the critical functions identified in Key Activity? • If so, have those critical functions that also involve the use of EPHI been identified? • Would different staff, facilities, or systems be needed to perform those functions? •Has the security of that EPHI in that alternative mode of operation been assured?		
7. Testing and Revision Procedure	• Implement procedures for periodic testing and revision of contingency plans. • Test the contingency plan on a predefined cycle (stated in the policy developed under Key Activity), if reasonable and appropriate. • Train those with defined plan responsibilities on their roles. • If possible, involve external entities (vendors, alternative site/service providers) in testing exercises. • Make key decisions regarding how the testing is to occur ("tabletop" exercise versus staging a real operational scenario including actual loss of capability). • Decide how to segment the type of testing based on the assessment of business impact and acceptability of sustained loss of service. Consider cost.	• How is the plan to be tested? • Does testing lend itself to a phased approach? • Is it feasible to actually take down functions/services for the purposes of testing? • Can testing be done during normal business hours or must it take place during off hours? • If full testing is infeasible, has a "tabletop" scenario (e.g., a classroom-like exercise) been considered? • How frequently is the plan to be tested (e.g., annually)? • When should the plan be revised?		
Evaluation 164.308(a)(8) **HIPAA Standard: 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.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Determine Whether Internal or External Evaluation Is Most Appropriate	• Decide whether the evaluation will be conducted with internal staff resources or external consultants. • Engage external expertise to assist the internal evaluation team where additional skills and expertise is determined to be reasonable and appropriate. • Use internal resources to supplement an external source of help, because these internal resources can provide the best institutional knowledge and history of internal policies and practices.	• Which staff has the technical experience and expertise to evaluate the systems? • How much training will staff need on security-related technical and nontechnical issues? • If an outside vendor is used, what factors should be considered when selecting the vendor, such as credentials and experience? • What is the budget for internal resources to assist with an evaluation? • What is the budget for external services to assist with an evaluation?		
2. Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule	• Use an evaluation strategy and tool that considers all elements of the HIPAA Security Rule and can be tracked, such as a questionnaire or checklist. • Implement tools that can provide reports on the level of compliance, integration, or maturity of a particular security safeguard deployed to protect EPHI. • If available, consider engaging corporate, legal, or regulatory compliance staff when conducting the analysis. • Leverage any existing reports or documentation that may already be prepared by [Organization's name] addressing compliance, integration, or maturity of a particular security safeguard deployed to protect EPHI.	• Have management, operational, and technical issues been considered? • Do the elements of each evaluation procedure (questions, statements, or other components) address individual, measurable security safeguards for EPHI? • Has [Organization's name] determined that the procedure must be tested in a few areas or systems? • Does the evaluation tool consider all standards and implementation specifications of the HIPAA Security Rule?		

3. Conduct Evaluation	• Determine, in advance, what departments and/or staff will participate in the evaluation. • Secure management support for the evaluation process to ensure participation. • Collect and document all needed information. Collection methods may include the use of interviews, surveys, and outputs of automated tools, such as access control auditing tools, system logs, and results of penetration testing. • Conduct penetration testing (where trusted insiders attempt to compromise system security for the sole purpose of testing the effectiveness of security controls), if reasonable and appropriate.	• If available, have staff members with knowledge of IT security been consulted and included in the evaluation team? • If penetration testing has been determined to be reasonable and appropriate, has specifically worded, written approval from senior management been received for any planned penetration testing? • Has the process been formally communicated to those who have been assigned roles and responsibilities in the evaluation process? • Has [Organization's name] explored the use of automated tools to support the evaluation process? • Has [Organization's name] employed automated tools to support the evaluation process?		
4. Document Results	• Document each evaluation finding, remediation options and recommendations, and remediation decisions. • Document known gaps between identified risks and mitigating security controls, and any acceptance of risk, including justification. • Develop security program priorities and establish targets for continuous improvement.	• Does the process support development of security recommendations? • In determining how best to display evaluation results, have written reports that highlight key findings and recommendations been considered? • If a written final report is to be circulated among key staff, have steps been taken to ensure that it is made available only to those persons designated to receive it?		
5. Repeat Evaluations Periodically	• Establish the frequency of evaluations, taking into account the sensitivity of the EPHI controlled by [Organization's name], its size, complexity, and environmental and/or operational changes (e.g., other relevant laws or accreditation requirements). • In addition to periodic reevaluations, consider repeating evaluations when environmental and operational changes are made to [Organization's name] that affects the security of EPHI (e.g., if new technology is adopted or if there are newly recognized risks to the security of the information).	• Do security policies specify that evaluations will be repeated when environmental and operational changes are made that affect the security of EPHI? • Do policies on frequency of security evaluations reflect any and all relevant federal or state laws which bear on environmental or operational changes affecting the security of EPHI? • Has [Organization's name] employed automated tools to support periodic evaluations?		
Business Associate Contracts and Other Arrangements (§ 164.308(b)(1)) **HIPAA Standard: A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on [Organization's name]'s behalf only if [Organization's name] obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Identify Entities that Are Business Associates under the HIPAA Security Rule	• Identify the individual or department who will be responsible for coordinating the execution of business associate agreements or other arrangements. • Reevaluate the list of business associates to determine who has access to EPHI in order to assess whether the list is complete and current. • Identify systems covered by the contract/agreement.	• Do the business associate agreements written and executed contain sufficient language to ensure that required information types will be protected? • Are there any new organizations or vendors that now provide a service or function on behalf of [Organization's name]? Such services may include the following: Claims processing or billing; Data analysis; Utilization review; Quality assurance; benefit management; Practice management; Re-pricing; Hardware maintenance; All other HIPAA-regulated functions • Have outsourced functions involving the use of EPHI been considered, such as the following: Actuarial services; Data aggregation; Administrative services; Accreditation; Financial services?		
2. Written Contract or Other Arrangement	• Document the satisfactory assurances required by this standard through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a). • Execute new or update existing agreements or arrangements as appropriate. • Identify roles and responsibilities	• Who is responsible for coordinating and preparing the final agreement or arrangement? • Does the agreement or arrangement specify how information is to be transmitted to and from the business associate? • Have security controls been specified for the business associate?		
3. Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met	• Maintain clear lines of communication. • Conduct periodic security reviews. • Establish criteria for measuring contract performance. • If the business associate is a governmental entity, update the memorandum of understanding or other arrangement when required by law or regulation or when reasonable and appropriate.	• What is the service being performed? • What is the outcome expected? • Is there a process for reporting security incidents related to the agreement? • Is there a process in place to periodically evaluate the effectiveness of business associate security controls? • Is there a process in place for terminating the contract if requirements are not being met and has the business associate been advised what conditions would warrant termination?		
4. Implement An Arrangement Other than a Business Associate Contract if Reasonable and Appropriate	• If [Organization's name] and its business associate are both governmental entities, use a memorandum of understanding or reliance on law or regulation that requires equivalent actions on the part of the business associate. • Document the law, regulation, memorandum, or other document that assures that the governmental entity business associate will implement all required safeguards for EPHI involved in transactions between the parties.	• Is [Organization's name]'s business associate a federal, state, or local governmental entity? • Is there a usual procedure for creating memoranda of understanding between the parties? • Has [Organization's name] researched and reviewed all law and regulation governing the use of EPHI by the governmental entity business associate?		

Physical Safeguards

Facility Access Controls 164.310(a)(1) HIPAA Standard: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Conduct an Analysis of Existing Physical Security Vulnerabilities	• Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities. • Assign degrees of significance to each vulnerability identified and ensure that proper access is allowed. • Determine which types of facilities require access controls to safeguard EPHI, such as: Data Centers; Peripheral equipment locations; IT staff offices; Workstation locations.	• If reasonable and appropriate, do nonpublic areas have locks and cameras? • Are workstations protected from public access or viewing? • Are entrances and exits that lead to locations with EPHI secured? • Do policies and procedures already exist regarding access to and use of facilities and equipment? • Do normal physical protections exist (locks on doors, windows, etc., and other means of preventing unauthorized access)?		
2. Identify Corrective Measures	• Identify and assign responsibility for the measures and activities necessary to correct deficiencies and ensure that proper access is allowed. • Develop and deploy policies and procedures to ensure that repairs, upgrades, and /or modifications are made to the appropriate physical areas of the facility while ensuring that proper access is allowed.	• Is a workforce member other than the security official responsible for facility/physical security? • Are facility access control policies and procedures already in place? Do they need to be revised? • What training will be needed for employees to understand the policies and procedures? • How will we document the decisions and actions? • Are we dependent on a landlord to make physical changes to meet the requirements?		
3. Develop a Facility Security Plan	• Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. • Implement appropriate measures to provide physical security protection for EPHI in a covered entity's possession. • Include documentation of the facility inventory, as well as information regarding the physical maintenance records and the history of changes, upgrades, and other modifications. • Identify points of access to the facility and existing security controls.	• Is there an inventory of facilities and existing security practices? • What are the current procedures for securing the facilities (exterior, interior, equipment, access controls, maintenance records, etc.)? • Is a workforce member other than the security official responsible for the facility plan?		
4. Develop Access Control and Validation Procedures	• Implement procedures to control and validate 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. • Implement procedures to provide facility access to authorized personnel and visitors, and exclude unauthorized persons.	• What are the policies and procedures in place for controlling access by staff, contractors, visitors, and probationary employees? • How many access points exist in each facility? Is there an inventory? • Is monitoring equipment necessary?		
5. Establish Contingency Operations Procedures	• 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.	• Who needs access to EPHI in the event of a disaster? • What is the backup plan for access to the facility and/or EPHI? • Who is responsible for the contingency plan for access to EPHI? • Who is responsible for implementing the contingency plan for access to EPHI in each department, unit, etc.? • Will the contingency plan be appropriate in the event of all types of potential disasters (fire, flood, earthquake, etc.)?		
6. Maintain Maintenance Records	• Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).	• Are records of repairs to hardware, walls, doors, and locks maintained? • Has responsibility for maintaining these records been assigned?		

Workstation Use 164.310(b) HIPAA Standard: 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.				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Identify Workstation Types and Functions or Uses	• Inventory workstations and devices. • Develop policies and procedures for each type of workstation and workstation device, identifying and accommodating their unique issues. • Classify workstations based on the capabilities, connections, and allowable activities for each workstation used.	• Do we have an inventory of workstation types and locations in my organization? • Who is responsible for this inventory and its maintenance? • What tasks are commonly performed on a given workstation or type of workstation? • Are all types of computing devices used as workstations identified along with the use of these workstations?		
2. Identify Expected Performance of Each Type of Workstation	• Develop and document policies and procedures related to the proper use and performance of workstations.	• How are workstations used in day-to-day operations? • What are key operational risks that could result in a breach of security?		

3. Analyze Physical Surroundings for Physical Attributes	• Ensure that any risks associated with a workstation's surroundings are known and analyzed for possible negative impacts. • Develop policies and procedures that will prevent or preclude unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and dispose of sensitive information as needed.	• Where are workstations located? • Is viewing by unauthorized individuals restricted or limited at these workstations? • Do changes need to be made in the space configuration? • Do employees understand the security requirements for the data they use in their day-to-day jobs?		
Workstation Security 164.310(c) **HIPAA Standard: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Identify All Methods of Physical Access to Workstations	• Document the different ways workstations are accessed by employees and nonemployees.	• Is there an inventory of all current workstation locations? • Are any workstations located in public areas? • Are laptops used as workstations?		
2. Analyze the Risk Associated with Each Type of Access	• Determine which type of access holds the greatest threat to security.	• Are any workstations in areas that are more vulnerable to unauthorized use, theft, or viewing of the data they contain? • What are the options for making modifications to the current access configuration?		
3. Identify and Implement Physical Safeguards for Workstations	• Implement physical safeguards and other security measures to minimize the possibility of inappropriate access to EPHI through workstations.	• What safeguards are in place, i.e., locked doors, screen barriers, cameras, guards? • Do any workstations need to be relocated to enhance physical security? • Have employees been trained on security?		
Device and Media Controls 164.310(d) (1) **HIPAA Standard: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Implement Methods for Final Disposal of EPHI	• Implement policies and procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored. • Determine and document the appropriate methods to dispose of hardware, software, and the data itself. • Assure that EPHI is properly destroyed and cannot be recreated.	• What data is maintained by [Organization's name], and where? • Is data on removable, reusable media such as tapes and CDs? • Is there a process for destroying data on hard drives and file servers? • What are the options for disposing of data on hardware? What are the costs?		
2. Develop and Implement Procedures for Reuse of Electronic Media	• Implement procedures for removal of EPHI from electronic media before the media are made available for reuse. • Ensure that EPHI previously stored on electronic media cannot be accessed and reused. • Identify removable media and their use. • Ensure that EPHI is removed from reusable media before they are used to record new information.	• Do policies and procedures already exist regarding reuse of electronic media (hardware and software)? • Is one individual and/or department responsible for coordinating the disposal of data and the reuse of the hardware and software? • Are employees appropriately trained on security and risks to EPHI when reusing software and hardware?		
3. Maintain Accountability for Hardware and Electronic Media	• Maintain a record of the movements of hardware and electronic media and any person responsible therefore. • Ensure that EPHI is not inadvertently released or shared with any unauthorized party. • Ensure that an individual is responsible for, and records the receipt and removal of, hardware and software with EPHI.	• Where is data stored (what type of media)? • What procedures already exist regarding tracking of hardware and software within the company? • If workforce members are allowed to remove electronic media that contain or may be used to access EPHI, do procedures exist to track the media externally? • Who is responsible for maintaining records of hardware and software?		
4. Develop Data Backup and Storage Procedures	• Create a retrievable exact copy of EPHI, when needed, before movement of equipment. • Ensure that an exact retrievable copy of the data is retained and protected to protect the integrity of EPHI during equipment relocation.	• Are backup files maintained offsite to assure data availability in the event data is lost while transporting or moving electronic media containing EPHI? • If data were to be unavailable while media are transported or moved for a period of time, what would the business impact be?		

Technical Safeguards

Access Control 164.312(a) (1) HIPAA Standard: 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).				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Analyze Workloads and Operations To Identify the Access Needs of All Users	• Identify an approach for access control. • Consider all applications and systems containing EPHI that should be available only to authorized users. • Integrate these activities into the access granting and management process.	• Have all applications/systems with EPHI been identified? • What user roles are defined for those applications/systems? • Where is the EPHI supporting those applications/systems currently housed (e.g., stand-alone PC, network)? • Are data and/or systems being accessed remotely?		
2. Identify Technical Access Control Capabilities	• Determine the access control capability of all information systems with EPHI	• How are the systems accessed (viewing data, modifying data, creating data)?		
3. Ensure that All System Users Have Been Assigned a Unique Identifier	• 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	• How should the identifier be established (length and content)? • Should the identifier be self-selected or randomly generated?		
4. Develop Access Control Policy	• Establish a formal policy for access control that will guide the development of procedures. • Specify requirements for access control that are both feasible and cost-effective for implementation.	• Have rules of behavior been established and communicated to system users? • How will rules of behavior be enforced?		
5. Implement Access Control Procedures Using Selected Hardware and Software	• Implement the policy and procedures using existing or additional hardware/software solution(s).	• Who will manage the access controls procedures? • Are current users trained in access control management? • Will user training be needed to implement access control procedures?		
6. Review and Update User Access	• Enforce policy and procedures as a matter of ongoing operations. • Determine if any changes are needed for access control mechanisms. • Establish procedures for updating access when users require the following: Initial access; Increased access; Access to different systems or applications than those they currently have	• Have new employees/users been given proper instructions for protecting data and systems? • What are the procedures for new employee/user access to data and systems? • Are there procedures for reviewing and, if appropriate, modifying access authorizations for existing users		
7. Establish an Emergency Access Procedure	• 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.	• When should the emergency access procedure be activated? • Who is authorized to make the decision? • Who has assigned roles in the process? • Will systems automatically default to settings and functionalities that will enable the emergency access procedure or will the mode be activated by the system administrator or other authorized individual?		
8. Automatic Logoff and Encryption and Decryption	• Consider whether the addressable implementation specifications of this standard are reasonable and appropriate: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.; Implement a mechanism to encrypt and decrypt EPHI.	• Are automatic logoff features available for any of [Organization's name]'s operating systems or other major applications? • If applications have been created or developed in-house, is it reasonable and appropriate to modify them to feature automatic logoff capability? • What period of inactivity prior to automatic logoff is reasonable and appropriate for [Organization's name]? • What encryption systems are available for [Organization's name]'s EPHI? • Is encryption appropriate for storing and maintaining EPHI ("at rest"), as well as while it is transmitted?		
9. Terminate Access if it is No Longer Required	• Ensure that access to EPHI is terminated if the access is no longer authorized.	• Are rules being enforced to remove access by staff members who no longer have a need to know because they have changed assignments or have stopped working for [Organization's name]?		

Audit Controls 164.312(b) HIPAA Standard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Determine the Activities that Will Be Tracked or Audited	• Determine the appropriate scope of audit controls that will be necessary in information systems that contain or use EPHI based on [Organization's name]'s risk assessment and other organizational factors. • Determine what data needs to be captured.	• Where is EPHI at risk in [Organization's name]? • What systems, applications, or processes make data vulnerable to unauthorized or inappropriate tampering, uses, or disclosures? • What activities will be monitored (e.g., creation, reading, updating, and/or deleting of files or records containing EPHI)? • What should the audit record include (e.g., user ID, event type/date/time)?		
2. Select the Tools that Will Be Deployed for Auditing and System Activity Reviews	• Evaluate existing system capabilities and determine if any changes or upgrades are necessary.	• What tools are in place? • What are the most appropriate monitoring tools for [Organization's name] (third party, freeware, or operating system-provided)? • Are changes/upgrades to information systems reasonable and appropriate?		
3. Develop and Deploy the Information System Activity Review/Audit Policy	• Document and communicate to the workforce the facts about [Organization's name]'s decisions on audits and reviews.	• Who is responsible for the overall audit process and results? • How often will audits take place? • How often will audit results be analyzed? • What is [Organization's name]'s sanction policy for employee violations? • Where will audit information reside (i.e., separate server)?		

4. Develop Appropriate Standard Operating Procedures	• Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports.	• How will exception reports or logs be reviewed? • Where will monitoring reports be filed and maintained? • Is there a formal process in place to address system misuse, abuse, and fraudulent activity? • How will managers and employees be notified, when appropriate, regarding suspect activity?		
5. Implement the Audit/System Activity Review Process	• Activate the necessary audit system. • Begin logging and auditing procedures.	• What mechanisms will be implemented to assess the effectiveness of the audit process (metrics)? • What is the plan to revise the audit process when needed?		
Integrity 164.312 (c) (1) **HIPAA Standard: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Identify All Users Who Have Been Authorized to Access EPHI	• Identify all approved users with the ability to alter or destroy data, if reasonable and appropriate. • Address this Key Activity in conjunction with the identification of unauthorized sources in Key Activity 2, below.	• How are users authorized to access the information? • Is there a sound basis established as to why they need the access? • Have they been trained on how to use the information? • Is there an audit trail established for all accesses to the information?		
2. Identify Any Possible Unauthorized Sources that May Be Able to Intercept the Information and Modify It	• Identify scenarios that may result in modification to the EPHI by unauthorized sources (e.g., hackers, disgruntled employees, business competitors). • Conduct this activity as part of your risk analysis	• What are likely sources that could jeopardize information integrity? • What can be done to protect the integrity of the information when it is residing in a system (at rest)? • What procedures and policies can be established to decrease or eliminate alteration of the information during transmission (e.g., encryption)?		
3. Develop the Integrity Policy and Requirements	• Establish a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps.	• Have the requirements been discussed and agreed to by identified key personnel involved in the processes that are affected? • Have the requirements been documented? • Has a written policy been developed and communicated to system users?		
4. Implement Procedures to Address These Requirements	• Identify and implement methods that will be used to protect the information from modification. • Identify and implement tools and techniques to be developed or procured that support the assurance of integrity.	• Are current audit, logging, and access control techniques sufficient to address the integrity of the information? • If not, what additional techniques can we apply to check information integrity (e.g., quality control process, transaction and output reconstruction)? • Can additional training of users decrease instances attributable to human errors?		
5. Implement a Mechanism to Authenticate EPHI	• Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner. • Consider possible electronic mechanisms for authentication such as: Error-correcting memory; Magnetic disk storage; Digital signatures; Check sum technology.	• Are the uses of both electronic and nonelectronic mechanisms necessary for the protection of EPHI? • Are appropriate electronic authentication tools available? • Are available electronic authentication tools interoperable with other applications and system components?		
6. Establish a Monitoring Process To Assess How the Implemented Process Is Working	• Review existing processes to determine if objectives are being addressed. • Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised.	• Are there reported instances of information integrity problems and have they decreased since integrity procedures have been implemented? • Does the process, as implemented, provide a higher level of assurance that information integrity is being maintained?		
Person or Entity Authentication 164.312 (d) **HIPAA Standard: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Determine 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.	• What authentication methods are available? • What are the advantages and disadvantages of each method? • What will it cost to implement the available methods in our environment? • Do we have trained staff who can maintain the system or do we need to consider outsourcing some of the support? • Are passwords being used? • If so, are they unique by individual?		
2. Evaluate Authentication Options Available	• 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, or a combination of two or more of the above approaches.	• What are the strengths and weaknesses of each available option? • Which can be best supported with assigned resources (budget/staffing)? • What level of authentication is appropriate based on our assessment of risk to the information/systems? • Do we need to acquire outside vendor support to implement the process?		

3. Select and Implement Authentication Option	• 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.	• Has necessary user and support staff training been completed? • Have formal authentication policy and procedures been established and communicated? • Has necessary testing been completed to ensure that the authentication system is working as prescribed? • Do the procedures include ongoing system maintenance and updates? • Is the process implemented in such a way that it does not compromise the authentication information (password file encryption, etc.)?		
Transmission Security (§ 164.312(e)(1)) **HIPAA Standard: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Identify Any Possible Unauthorized Sources that May Be Able to Intercept and/or Modify the Information	• Identify scenarios that may result in modification of the EPHI by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors).	• What measures exist to protect EPHI in transmission? • Is there an auditing process in place to verify that EPHI has been protected against unauthorized access during transmission? • Are there trained staff members to monitor transmissions?		
2. Develop and Implement Transmission Security Policy and Procedures	• Establish a formal (written) set of requirements for transmitting EPHI. • Identify methods of transmission that will be used to safeguard EPHI. • Identify tools and techniques that will be used to support the transmission security policy. • Implement procedures for transmitting EPHI using hardware and/or software, if needed.	• Have the requirements been discussed and agreed to by identified key personnel involved in transmitting EPHI? • Has a written policy been developed and communicated to system users?		
3. Implement Integrity Controls Implementation Specification	• Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.	• What measures are planned to protect EPHI in transmission? • Is there assurance that information is not altered during transmission?		
4. Implement Encryption	• Implement a mechanism to encrypt EPHI whenever deemed appropriate.	• Is encryption reasonable and appropriate for EPHI in transmission? • Is encryption needed to effectively protect the information? • Is encryption feasible and cost-effective in this environment? • What encryption algorithms and mechanisms are available? • Does [Organization's name] have the appropriate staff to maintain a process for encrypting EPHI during transmission? • Are staff members skilled in the use of encryption?		

Organizational Requirements

Business Associate Contracts or Other Arrangements (§ 164.314(a)(1)) HIPAA Standard: (i) The contract or other arrangement between [Organization's name] and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if [Organization's name] knew of a pattern of an 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 [Organization's name] took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—(A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Contract Must Provide that Business Associates Adequately Protect EPHI	• Contracts between covered entities and business associates must provide that business associates will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that the business associate creates, receives, maintains, or transmits on behalf of [Organization's name]. • May consider asking the business associate to conduct a risk assessment that addresses administrative, technical, and physical risks, if reasonable and appropriate.	• Does the written agreement between [Organization's name] and the business associate address the applicable functions related to creating, receiving, maintaining, and transmitting EPHI that the business associate is to perform on behalf of [Organization's name]?		
2. Contract Must Provide that Business Associate's Agents Adequately Protect EPHI	• Contracts between covered entities and business associates must provide that any agent, including a subcontractor, to whom the business associate provides such information agrees to implement reasonable and appropriate safeguards to protect it.	• Does the written agreement address the issue of EPHI access by subcontractors and other agents of the business associate?		
3. Contract Must Provide that Business Associate	• Contracts between covered entities and business associates must provide that business associates will report to [Organization's name] any security incident of which it becomes aware. • Establish a reporting mechanism and a process for the business associate to use in the event of a security incident.	• Is there a procedure in place for reporting of incidents by business associates? • Have key business associate staff that would be the point of contact in the event of a security incident been identified?		
4. Contract Must Provide that Business Associate Will Authorize Termination of the Contract if it has been Materially Breached	• Contracts between covered entities and business associates must provide that the business associate will authorize termination of the contract by [Organization's name] if [Organization's name] determines that the business associate has violated a material term of the contract. • Establish in the written agreement with business associates the circumstances under which a violation of agreements relating to the security of EPHI constitutes a material breach of the contract. • Terminate the contract if: [Organization's name] learns that the business associate has violated the contract or materially breached it, and; It is not possible to take reasonable steps to cure the breach or end the violation, as applicable. • If terminating the contract is not feasible, report the problem to the Secretary of HHS.	• Have standards and thresholds for termination of the contract been included in the contract?		
5. Government Entities May Satisfy Business Associate Contract Requirements through Other Arrangements	• If [Organization's name] and business associate are both governmental entities, consult § 164.314 (a)(2)(ii) of the Security Rule. • If both entities are governmental entities, [Organization's name] is in compliance with § 164.314 (a)(1) if: It executes a Memorandum of Understanding (MOU) with the business associate that contains terms that accomplish the objectives of § 164.314(a)(2)(i), or; Other law (including regulations adopted by [Organization's name] or its business associate) contains requirements applicable to the business associate that accomplish the objectives of § 164.314(a)(2)(i).	• Do the arrangements provide protections for EPHI equivalent to those provided by [Organization's name]'s business associate contracts? • If termination of the MOU is not possible due to the nature of the relationship between [Organization's name] and the business associate, are other mechanisms for enforcement available, reasonable, and appropriate?		
6. Other Arrangements for Covered Entities and Business Associates.	• If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in §160.103 to a covered entity, [Organization's name] may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of § 164.314(a)(2)(i), provided that [Organization's name] attempts in good faith to obtain satisfactory assurances as required by § 164.314(a)(2)(ii)(A), and documents the attempt and the reasons that these assurances cannot be obtained. • [Organization's name] may omit from its other arrangements authorization of the termination of the contract by [Organization's name], as required by § 164.314(a)(2)(i)(D), if such authorization is inconsistent with the statutory obligations of [Organization's name] or its business associate.	• Has [Organization's name] made a good faith attempt to obtain satisfactory assurances that the security standards required by this section are met? • Are attempts to obtain satisfactory assurances and the reasons assurances cannot be obtained documented? • Does [Organization's name] or its business associate have statutory obligations which require removal of the authorization of termination requirement?		

Requirements for Group Health Plans (§ 164.314(b)(1)) HIPAA Standard: 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.				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Amend Plan Documents of Group Health Plan to Address Plan Sponsor's Security of EPHI	• Amend plan documents to incorporate provisions to require the plan sponsor (e.g., an entity that sponsors a health plan) to implement administrative, technical, and physical safeguards that will reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits on behalf of the group health plan.	• Does the plan sponsor fall under the exception described in the standard? • Do the plan documents require the plan sponsor to reasonably and appropriately safeguard EPHI?		
2. Amend Plan Documents of Group Health Plan to Address Adequate Separation	• Amend plan documents to ensure that the adequate separation between the group health plan and plan sponsor required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.	• Do plan documents address the obligation to keep EPHI secure with respect to the plan sponsor's employees, classes of employees, or other persons who will be given access to EPHI?		
3. Amend Plan Documents of Group Health Plan to Address Security of EPHI Supplied to Plan Sponsors' Agents and Subcontractors	• Amend plan documents to incorporate provisions to require the plan sponsor to ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate security measures to protect the EPHI.	• Do the plan documents of the group health plan address the issue of subcontractors and other agents of the plan sponsor implementing reasonable and appropriate security measures?		
4. Amend Plan Documents of Group Health Plans to Address Reporting of Security Incidents	• Amend plan documents to incorporate provisions to require the plan sponsor to report to the group health plan any security incident of which it becomes aware. • Establish specific policy for security incident reporting. • Establish a reporting mechanism and a process for the plan sponsor to use in the event of a security incident.	• Is there a procedure in place for security incident reporting? • Are procedures in place for responding to security incidents?		

Policies and Procedures and Documentation Requirements

Policies and Procedures (§ 164.316(a)) HIPAA Standard: 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 may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Create and Deploy Policies and Procedures	• Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule. • Periodically evaluate written policies and procedures to verify that: Policies and procedures are sufficient to address the standards, implementation specifications, and other requirements of the HIPAA Security Rule.; Policies and procedures accurately reflect the actual activities and practices exhibited by [Organization's name], its staff, its systems and its business associates.	• Are reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule in place? • Are policies and procedures reasonable and appropriate given: the size, complexity, and capabilities of [Organization's name]; [Organization's name]'s technical infrastructure, hardware, and software security capabilities; the costs for security measures; and the probability and criticality of potential risks to EPHI? • Do procedures exist for periodically reevaluating the policies and procedures, updating them as necessary?		
2. Update Documentation of Policy and Procedures	• Change policies and procedures as is reasonable and appropriate, at any time, provided that the changes are documented and implemented in accordance with the requirements of the HIPAA Security Rule.	• Should HIPAA documentation be updated in response to periodic evaluations, following security incidents, and/or after acquisitions of new technology or new procedures? As policies and procedures are changed, are new versions made available and are workforce members appropriately trained?		
Documentation (§ 164.316(b)(1)) **HIPAA Standard: (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 of the action, activity, or assessment.**				
Key Activities	**Descriptions**	**Questions to Answer**	**How is the Standard Implemented?**	**Departmental Implementation**
1. Draft, Maintain and Update Required Documentation	• Document the decisions concerning the management, operational, and technical controls selected to mitigate identified risks. • Written documentation may be incorporated into existing manuals, policies, and other documents, or may be created specifically for the purpose of demonstrating compliance with the HIPAA Security Rule.	• Are all required policies and procedures documented? • Should HIPAA Security Rule documentation be maintained by the individual responsible for HIPAA Security implementation? • Should HIPAA Security documentation updated in response to periodic evaluations, following security incidents, and/or after acquisitions of new technology or new procedures?		
2. Retain Documentation for at Least Six Years	• Retain required documentation of policies, procedures, actions, activities or assessments required by the HIPAA Security Rule for six years from the date of its creation or the date when it last was in effect, whichever is later.	• Have documentation retention requirements under HIPAA been aligned with [Organization's name]'s other data retention policies?		
3. Assure that Documentation is Available to those Responsible for Implementation	• Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	• Is the location of documentation known to all staff that needs to access it? • Is availability of the documentation made known as part of education, training and awareness activities?		
4. Update Documentation as Required	• Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the EPHI.	• Is there a version control procedure that allows verification of the timeliness of policies and procedures, if reasonable and appropriate? • Is there a process for soliciting input into updates of policies and procedures from staff, if reasonable and appropriate?		