

ADMINISTRATIVE SAFEGUARDS		CFR	Sample Audit Questions from CMS Security Series	Agency Policy Description and Location	Comments/Questions
Security Management Process	164.308(a)(1)				
Risk Analysis (R)	164.308(a)(1)	(A) Risk analysis (Required). 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.	1) Identify potential security risks, 2) Determine probability of occurrence and magnitude of risks.		
Risk Management (R )	164.308(a)(1)	(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306 (a)		
Sanction Policy (R)	164.308(a)(1)	(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	1) Sanction policy and procedure, 2) signed statement of adherence to security policy and a prerequisite that acknowledge disciplinary actions for violations up to and including termination, 3) policy contains examples, 4) adjust disciplinary action based on severity of violation?		
Information System Activity Review (R )	164.308(a)(1)	(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	1) What are the audit and activity review functions of the current information systems 2) Are the IS functions adequately used and monitored to promote continual awareness of IS activity? 3) What logs or reports are generated by the Info. System? 4) Is there a policy that establishes what reviews will be conducted? 5) Is there a procedure that describes the specifics of the reviews?		
Assigned Security Responsibility (R )	164.308(a)(2)	(2) Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity		
Workforce Security	164.308(a)(3)	(3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Purpose is to ensure workforce members have appropriate access to IS EPHI		
Authorization and/or Supervision (A)	164.308(a)(3)	(A) Authorization and/or supervision (Addressable). 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.	What process or criteria are used to determine who can have access to EPHI (i.e. job descriptions used, who makes the determination, is office so small that global access is okay?)		

ADMINISTRATIVE SAFEGUARDS	CFR	Sample Audit Questions from CMS Security Series	Agency Policy Description and Location	Comments/Questions
Workforce Clearance Procedure (A)	164.308(a)(3) (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	A screening procedure for allowing access to EPHI		
Termination Procedures (A)	164.308(a)(3) (C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Procedures for termination access to PHI when employment ends.		
Information Access Management	164.308(a)(4) <b>(4)(i) Standard: 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.</b>			
Isolating Health Care Clearinghouse Functions (R )	164.308(a)(4) (A) Isolating health care clearinghouse functions (Required). 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.	Only applies if a health care clearinghouse is part of a larger organization.		
Access Authorization (A)	164.308(a)(4) (B) Access authorization (Addressable). 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.	How is authorization documented? 2) Are policies and procedures for granting access consistent with the Privacy Rule? 3) Have appropriate authorization and clearance procedures, as specified in workforce security, been performed prior to granting access? 4) Are access rules specific to applications and business requirements? For example, do different workforce members require different levels of access based on job function? 5) Is there a technical process in place such as creating unique user name and an authentication process, when granting access to a workforce member?		
Access Establishment and Modification (A)	164.308(a)(4) (C) Access establishment and modification (Addressable). 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.	1) Are policies and procedures in place for establishing access and modifying access? 2) Are system access policies and procedures documented and updated as necessary? 3) Do members of management or other workforce members periodically review the list of persons with access to EPHI to ensure they are valid and consistent with those authorized?		
Security Awareness and Training	164.308(a)(5) <b>(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).</b>	Periodic retraining should be given whenever environmental or operational changes affect the security of EPHI. Changes may include: New or updated policies and procedures; new or upgraded software or hardware; new security technology; or even changes in the security rule.		
Security Reminders (A)	164.308(a)(5) (A) Security reminders (Addressable). Periodic security updates.	Such as: agenda items at meetings, focused reminders posted in affected areas, and/or formal training		

ADMINISTRATIVE SAFEGUARDS		CFR	Sample Audit Questions from CMS Security Series	Agency Policy Description and Location	Comments/Questions
Protection from Malicious Software (A)	164.308(a)(5)	(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	Procedures to guard against, detect and report malicious software.		
Log-in Monitoring (A)	164.308(a)(5)	(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	If log-in monitoring is reasonable and appropriate safeguard, there must be procedures for monitoring log-in attempts and reporting discrepancies.		
Password Management (A)	164.308(a)(5)	(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	1) Are there policies in place that prevent workforce members from sharing passwords with others? 2) Is the workforce advised to commit their passwords to memory? 3) Are common sense precautions taken, such as not writing passwords down and leaving them in areas that are visible or accessible to others?		
Security Incident Procedures	164.308(a)(6)	<b>(6)(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.</b>	Identify, respond, mitigate, document suspected or known security incidents and document outcomes.		
Response and Reporting (R)	164.308(a)(6)	(ii) Implementation specification: Response and Reporting (Required). 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	1) Are policies and procedures developed and implemented to address security incidents? 2) Do the security incident policies and procedures list possible types of security incidents and the response for each? 3) Do the security incident policies and procedures identify to whom security incidents must be reported? see list below of examples		
Contingency Plan	164.308(a)(7)	<b>(7)(i) Standard: Contingency plan. 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.</b>	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 EPHI. Should include plan for physical access (see facility access control, contingency operations)		
Data Backup Plan (R)	164.308(a)(7)	A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	1) What is the EPHI that must be backed up? 2) Does the plan include all important sources of data such as patient accounting systems, emir, health maintenance and case management information, digital recordings of diagnostic images, electronic test results, or any other electronic documents created or used? 3) Has the organization considered the various methods of backups, including tape, disk, or CD? 4) Does the backup plan include storage of backups in a safe, secure place? 5) Is the organization's frequency of backups appropriate for its environment?		

ADMINISTRATIVE SAFEGUARDS		CFR	Sample Audit Questions from CMS Security Series	Agency Policy Description and Location	Comments/Questions
Disaster Recovery Plan (R)	164.308(a)(7)	(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.	1) Does the disaster recovery plan address issues specific to the covered entity's operating environment? 2) Does the plan address what data is to be restored? 3) Is a copy of the disaster recovery plan readily accessible at more than one location?		
Emergency Mode Operation Plan ®	164.308(a)(7)	(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	1) Does the organization's plan balance the need to protect the data with the organization's need to access the data? 2) Will alternative security measures be used to protect the EPHI? 3) Does the emergency mode operation plan include possible manual procedures for security protection that can be implemented as needed? 4) Does the emergency mode operation plan include telephone numbers and contact names for all persons that must be notified in the event of a disaster, as well as roles and responsibilities of those people involved in the restoration process?		
Testing and Revision Procedures (A)	164.308(a)(7)	(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.	1) Are the processes for restoring data from backups, disaster recovery and emergency mode operation documented? 2) Do those responsible for performing contingency planning tasks understand their responsibilities? 3) Have those responsible actually performed a test of the procedures? 4) Have the results of each test been documented and any problems with the test reviewed and corrected?		
Applications and Data Criticality Analysis (A)	164.308(a)(7)	(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.	Identify software applications (data applications that store, maintain, or transmit EPHI) and determine how important each is to patient care or business needs, in order to prioritize for data backup, disaster recovery and/or emergency operation plans. A prioritized list of specific applications and data will help determine which applications or information systems get restored first and/or which must be available at all times.		
Evaluation (R)	164.308(a)(8)	<b>(8) Standard: 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, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.</b>	1) Subsequent periodic evaluations must be performed in response to environmental or operational changes that affect the security of EPHI. 2) Should occur annually or every 2 years, or possibly when a known change or security incident has occurred. 3) The evaluation must include the technical and non-technical aspects of the security program. 4) Should be documented		

ADMINISTRATIVE SAFEGUARDS	CFR	Sample Audit Questions from CMS Security Series	Agency Policy Description and Location	Comments/Questions
Business Associate Contracts and Other Arrangements	164.308(b)(1) <b>(b)(1) Standard: Business associate contracts and other arrangements. A covered entity, in accordance with §164.306, 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</b>			
Written Contract or Other Arrangement (R )	164.308(b)(1) (4) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).	1) Have all business associates been identified? 2) Do business associate contracts or agreements include privacy and security requirements? See below for a list of business associate examples.		

**Examples of security incidents:**

- \*Stolen or otherwise inappropriately obtained passwords that are used to access EPHI
- \*Corrupted backup tapes that do not allow restoration of EPHI
- \*Virus attacks that interfere with the operations of information systems with EPHI
- \*Physical break-ins leading to the theft of media with EPHI
- \*Failure to terminate the account of a former employee that is then used by an unauthorized user- to access informatin systems with EPHI
- \*Providing media with EPHI, such as a PC hard drive or laptop, to another user who is not authorized to- access the EPHI prior to removing the EPHI stored on the media

**Examples of Business Associates**

- clearinghouses
- medical billing services
- vendors of hardware and software
- external consultants
- lawyers
- transcription contractors
- others who have access to EPHI