MALVERNGROUP

HIPAA Security Audit PrepBook

Version 1.0, Released August 26, 2012

This document is derived entirely from the HIPAA Audit Protocols published at http://ocrnotifications.hhs.gov/hipaa.html on June 26, 2012.

MalvernGroup has endeavored to make no changes to the content or the original OCR publication and to represent the information faithfully: any errors, notes included by the original Protocol authors or other discrepancies are included without comment.

MalvernGroup has analyzed and interpreted the published OCR HIPAA Audit Protocols (the Protocols) to identify documentation that may be requested in an OCR Audit of a Covered Entity's or Business Associate's compliance with the HIPAA Security Rule.

While MalvernGroup has attempted to identify all documents that may be requested, on the basis of the Protocols and on the basis of other reasonable requests which are not part of the published Protocols, MalvernGroup does not warrant that all documents that may be requested have been identified in this PrepBook. MalvernGroup does not warrant that a Covered Entity/Business Associate that has produced all documents identified in this PrepBook will be in compliance with any HIPAA rule or that a Covered Entity/Business Associate will not receive negative audit comments.

This document is based on the OCR's first release of the HIPAA Security protocols and MalvernGroup's interpretations. Please notify us of any discrepancies you may find and we will consider them in an updated version.

This document does not contain legal advice.

This document was authored and reviewed by:
Carl N. Abramson and Susan A. Miller J.D.

MALVERNGROUP

Table of Contents

About this Document 7

Legal Aspects of OCR HIPAA Audit Protocol 7

Management Interviews 7

Informal Policies and Procedures 7

Evidence of compliance 8

Duplication of Requested Evidence 8

Terms and phrases used in OCR HIPAA Audit Protocol 8

Suggested Practical Evidence 9

Columns added by MalvernGroup 10

Audit Protocol 11

Conduct Risk Assessment 11

Acquire IT Systems and Services 12

Develop and Deploy the Information System Activity Review Process 13

Development and Implement a Sanction Policy 14

Select a Security Official To Be Assigned Responsibility for HIPAA Security 15

Assign and Document the Individual's Responsibility 16

Establish Clear Job Description and Responsibilities....17
Establish Criteria and Procedures for Hiring and Assigning Tasks....18
Establish a Workforce Clearance Procedures....19
Establish Termination Procedures....20
Implement Policies and Procedures for Authorizing Access....22
Implement Policies and Procedures for Access Establishment and Modification....23
Isolate Healthcare Clearinghouse Functions....24
Evaluate Existing Security Measures Related to Access Controls....25
Develop and Approve a Training Strategy and a Plan....26
Develop and Approve a Training Strategy and a Plan....27
Protection from Malicious Software; Log-in Monitoring; and Password Management....28
Develop Appropriate Awareness and Training Content, Materials, and Methods....29
Implement the Training....30
Implement Security Reminders....31
Monitor and Evaluate Training Plan....32
Develop and Implement Procedures to Respond to and Report Security Incidents....33
Develop and Implement Procedures to Respond to and Report Security Incidents....34
Develop Contingency Planning Policy....35

Data Backup Plan and Disaster Recovery Plan 36
Develop and Implement an Emergency Mode Operation Plan 37
Testing and Revision Procedure 38
Identify Preventive Measures 39
Develop Recovery Strategy 40
Data Backup Plan and Disaster Recovery Plan 41
Determine Whether Internal or External Evaluation Is Most Appropriate 42
Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule 43
Conduct Evaluation 44
Document Results 45
Repeat Evaluations Periodically 46
Written Contract or Other Arrangement 47
Implement An Arrangement Other than a Business Associate Contract if Reasonable and Appropriate 48
Conduct an Analysis of Existing Physical Security Vulnerabilities 49
Develop a Facility Security Plan 50
Establish Contingency Operations Procedures 51
Establish Contingency Operations Procedures 52
Maintain Maintenance Records 53

Identify Workstation Types and Functions or Uses....54
Identify Expected Performance of Each Type of Workstation....55
Analyze Physical Surroundings for Physical Attributes....56
Identify All Methods of Physical Access to Workstations....57
Identify and Implement Physical Safeguards for Workstations....58
Implement Methods for Final Disposal of ePHI....59
Maintain Accountability for Hardware and Electronic Media....60
Develop Data Backup and Storage Procedures....61
Develop Data Backup and Storage Procedures....63
Develop and Implement Procedures for Reuse of Electronic Media....65
Encryption and Decryption....66
Analyze Workloads and Operations to Identify the Access Needs of All Users....67
Identify Technical Access Control Capabilities....68
Ensure that All System Users Have Been Assigned a Unique Identifier....69
Develop Access Control Policy....70
Implement Access Control Procedures Using Selected Hardware and Software....71
Implement Access Control Procedures Using Selected Hardware and Software....72
Implement Access Control Procedures Using Selected Hardware and Software....73

Review and Update User Access 74
Establish an Emergency Access Procedure 75
Establish an Emergency Access Procedure 76
Automatic Logoff 77
Terminate Access if it is No Longer Required 78
Determine the Activities that Will be Tracked or Audited 79
Select the Tools that Will be Deployed for Auditing and System Activity Reviews 80
Develop and Deploy the Information System Activity Review/Audit Policy 81
Develop Appropriate Standard Operating Procedures 82
Identify All Users Who Have Been Authorized to Access ePHI 83
Implement Procedures to Address These Requirements 84
Implement a Mechanism to Authenticate ePHI 85
Determine Authentication Applicability to Current Systems/Applications 86
Evaluate Authentication Methods Available 87
Select and Implement Authentication Option 88
Select and Implement Authentication Option 89
Develop and Implement Transmission Security Policy and Procedures 90
Version History 91

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification	Requested Evidence	Available Y/N	Document ID	Owner	Location

§164.308	§164.308(a)(3) **Workforce Security** - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	**Establish Clear Job Description and Responsibilities**	Inquire of management as to whether a formal document is in place identifying levels of access to information systems that houses ePHI.
			
			Obtain and review formal documentation and evaluate the content in relation to the specified criteria to determine that levels of access are granted based on business need.
			
			Obtain and review evidence that the formal documentation establishing levels of access is appropriately approved and communicated.
			
			Obtain and review relevant job descriptions and evaluate the content in relation to the specified performance criteria and determine that roles and responsibilities are defined and correlate with job function.
			
			If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.
			
			-end of audit procedure-
				Addressable	• A formal document identifying levels of access[1] to information systems that houses ePHI based on business need
					• Formal documentation establishing levels of access is appropriately approved
					• Formal documentation establishing levels of access is appropriately communicated
					• Appropriate level of access to ePHI is defined in ***all*** job descriptions
					• If the covered entity has chosen not to fully implement this specification:
					  ○ documentation on where they have chosen not to fully implement this specification
					  ○ rationale for not fully implementing this specification				

[1] MalvernGroup interprets “levels of access” to represent the appropriate ePHI that is needed to perform a workforce members work.

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification	Requested Evidence	Available Y/N	Document ID	Owner	Location
§164.308	§164.308(a)(3) **Workforce Security** - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	**Establish Criteria and Procedures for Hiring and Assigning Tasks**	Inquire of management as to whether staff members have the necessary knowledge, skills, and abilities to fulfill particular roles. Obtain and review formal documentation and evaluate the content in relation to the specified criteria. Obtain and review documentation demonstrating that management verified the required experience/qualifications of the staff (per management policy). If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so. -end of audit procedure-	Addressable	• Policy that requires workforce members to have the knowledge, experience and qualifications as defined in job descriptions or roles that include the responsibility to access ePHI				
					• Procedures that ensure that new hires and staff have the knowledge, experience and qualifications as defined in job descriptions or roles that include the responsibility to access ePHI				
					• Documentation that demonstrates management has verified the required experience/qualifications of the staff per policy; see Workforce Clearance Key Activity below				
					• Evidence of compliance with policy and any criteria contained therein.				
					• If the covered entity has chosen not to fully implement this specification: o documentation on where they have chosen not to fully implement this specification o rationale for not fully implementing this specification				

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification	Requested Evidence	Available Y/N	Document ID	Owner	Location
§164.308	§164.308(a)(3) **Workforce Security** - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	**Establish a Workforce Clearance Procedures**	Inquire of management as to whether procedures exist for granting access to ePHI. Obtain and review policy and procedures and evaluate the content in relation to the relevant specified performance criteria. Obtain and review evidence of approval or verification of access to ePHI. If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so. -end of audit procedure-	Addressable	• Policies and procedures for granting access to ePHI that ensure that all members of the workforce have appropriate access and prevent those workforce members who do not have access from obtaining access				
					• Evidence of compliance with policy and any criteria contained therein ○ ***Documented policy defining "appropriate": the qualifications workforce members are required to meet in order to be authorized to access ePHI (PHI)*** ○ ***Evidence demonstrating that workforce members meet criteria prior to their access to ePHI (PHI)***				
					• Evidence of approval and verification of access to ePHI				
					• If the covered entity has chosen not to fully implement this specification: ○ documentation on where they have chosen not to fully implement this specification ○ rationale for not fully implementing this specification				