

# HIPAA Security Final Rule

Standards	Sections	Implementation Specifications R=Required A=Addressable
<b>ADMINISTRATIVE SAFEGUARDS</b>		
<b>Security Management Process</b>	164.308(a)(1)(i)	
Risk Analysis (R)	164.308(a)(1)(ii)(A)	R
Risk Management (R)	164.308(a)(1)(ii)(B)	R
Sanction Policy (R)	164.308(a)(1)(ii)(C)	R
Information System Activity Review (R)	164.308(a)(1)(ii)(D)	R
<b>Assigned Security Responsibility</b>	164.308(a)(2)	R
<b>Workforce Security</b>	164.308(a)(3)(i)	R
Authorization and/or Supervision (A)	164.308(a)(3)(ii)(A)	A
Workforce Clearance Procedure (A)	164.308(a)(3)(ii)(B)	A
Termination Procedures (A)	164.308(a)(3)(ii)(C)	A
<b>Information Access Management</b>	164.308(a)(4)(i)	R
Isolating Health care Clearinghouse Function (R)	164.308(a)(4)(ii)(A)	R
Access Authorization (A)	164.308(a)(4)(ii)(B)	A
Access Establishment and Modification (A)	164.308(a)(4)(ii)(C)	A
<b>Security Awareness and Training</b>	164.308(a)(5)(i)	R
Security Reminders (A)	164.308(a)(5)(ii)(A)	A
Protection from Malicious Software (A)	164.308(a)(5)(ii)(B)	A
Log-in Monitoring (A)	164.308(a)(5)(ii)(C)	A
Password Management (A)	164.308(a)(5)(ii)(D)	A
<b>Security Incident Procedures</b>	164.308(a)(6)(i)	R
Response and Reporting (R)	164.308(a)(6)(ii)	R
<b>Contingency Plan</b>	164.308(a)(7)(i)	R
Data Backup Plan (R)	164.308(a)(7)(ii)(A)	R
Disaster Recovery Plan (R)	164.308(a)(7)(ii)(B)	R
Emergency Mode Operation Plan (R)	164.308(a)(7)(ii)(C)	R
Testing and Revision Procedure (A)	164.308(a)(7)(ii)(D)	A
Applications and Data Criticality Analysis (A)	164.308(a)(7)(ii)(E)	A
<b>Evaluation</b>	164.308(a)(8)	R
<b>Business Associate Contracts and Other Arrangements</b>	164.308(b)(1)	R
Written Contract or Other Arrangement (R)	164.308(b)(4)	R
<b>PHYSICAL SAFEGUARDS</b>		
<b>Facility Access Controls</b>	164.310(a)(1)	R
Contingency Operations (A)	164.310(a)(2)(i)	A
Facility Security Plan (A)	164.310(a)(2)(ii)	A
Access Control and Validation Procedures (A)	164.310(a)(2)(iii)	A
Maintenance Records (A)	164.310(a)(2)(iv)	A
<b>Workstation Use</b>	164.310(b)	R
<b>Workstation Security</b>	164.310(c)	R
<b>Device and Media Controls</b>	164.310(d)(1)	R
Disposal (R)	164.310(d)(2)(i)	R
Media Re-use (R)	164.310(d)(2)(ii)	R
Accountability (A)	164.310(d)(2)(iii)	A
Data Backup and Storage (A)	164.310(d)(2)(iv)	A
<b>TECHNICAL SAFEGUARDS (see § 164.312)</b>		
<b>Access Control</b>	164.312(a)(1)	R
Unique User Identification (R)	164.312(a)(2)(i)	R
Emergency Access Procedure (R)	164.312(a)(2)(ii)	R
Automatic Logoff (A)	164.312(a)(2)(iii)	A
Encryption and Decryption (A)	164.312(a)(2)(iv)	A
<b>Audit Controls</b>	164.312(b)	R
<b>Integrity</b>	164.312(c)(1)	R
Mechanism to Authenticate Electronic Protected Health Information (A)	164.312(c)(2)	A
<b>Person or Entity Authentication</b>	164.312(d)	R
<b>Transmission Security</b>	164.312(e)(1)	R
Integrity Controls (A)	164.312(e)(2)(i)	A
Encryption (A)	164.312(e)(2)(ii)	A

# HIPAA Security Final Rule

<b>Organizational Requirements (see § 164.314)</b>		
<b>Business associate contracts or other arrangements.</b>	164.314(a)(1)	R
Business associate contracts.	164.314(a)(2)(i)	R
Other arrangements.	164.314(a)(2)(ii)	R
<b>Requirements for group health plans.</b>	164.314(b)(1)	R
Amend Group Health Plan Documents	164.314(b)(2)	R
Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;	164.314(b)(2)(i)	R
Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;	164.314(b)(2)(ii)	R
Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and	164.314(b)(2)(iii)	R
Report to the group health plan any security incident of which it becomes aware.	164.314(b)(2)(iv)	R
<b>Policies and Procedures and Documentation Requirements (see § 164.316)</b>		
<b>Policies and procedures.</b>	164.316(a)	R
<b>Documentation.</b>	164.316(b)(1)	
Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and	164.316(b)(1)(i)	R
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.	164.316(b)(1)(ii)	R
Time limit (Required).	164.316(b)(2)(i)	R
Availability (Required).	164.316(b)(2)(ii)	R
Updates (Required).	164.316(b)(2)(iii)	R