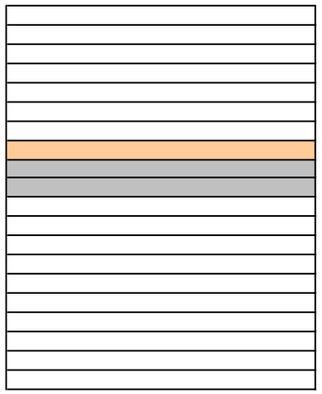
Item	HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Requirement Description	Solution	Full Regulatory Text	Compliance Level	Current Practice Findings & ePHI Assets at Risk (reference inventory items individually)
SECURITY STANDARDS: GENERAL RULES								
1	164.306(a)	**Ensure Confidentiality, Integrity & Availability**	-	Ensure CIA and protect against threats	-	(a) General requirements. Covered entities must do the following:		
2	164.306(b)	**Flexibility of Approach**	-	Reasonably consider factors in security compliance	-	(b) Flexibility of approach.		
3	164.306(c)	**Standards**	-	CEs must comply with standards	-	(c) Standards. A covered entity must comply with the standards as provided in this		
4	164.306(d)	**Implementation Specifications**	-	Required and Addressable Implementation	-	(d) Implementation specifications.		
5	164.306(e)	**Maintenance**	-	Ongoing review and modification of security measures	-	(e) Maintenance. Security measures implemented to comply with standards and		
ADMINISTRATIVE SAFEGUARDS								
6	164.308(a)(1)(i)	**Security Management Process**	-	P&P to manage security violations	P&P	Implement policies and procedures to prevent, detect, contain and correct security		
7	164.308(a)(1)(ii)(A)	Risk Analysis	**Required**	Conduct vulnerability assessment	Assessment	Conduct an accurate and thorough assessment of the potential risks and		
8	164.308(a)(1)(ii)(B)	Risk Management	**Required**	Implement security measures to reduce risk of	Measures	Implement security measures sufficient to reduce risks and vulnerabilities to a		
9	164.308(a)(1)(ii)(C)	Sanction Policy	**Required**	Worker sanction for P&P violations	P&P	Apply appropriate sanctions against workforce members who fail to comply with the		
10	164.308(a)(1)(ii)(D)	Information System Activity Review	**Required**	Procedures to review system activity	Procedures	Implement procedures to regularly review records of information system activity, such		
11	164.308(a)(2)	**Assigned Security Responsibility**	-	Identify security official responsible for P&P	Assignment	Identify the security official who is responsible for the development and		
12	164.308(a)(3)(i)	**Workforce Security**	-	Implement P&P to ensure approp PHI access	P&P	Implement policies and procedures to ensure that all members of its workforce have		
13	164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Addressable	Authorization/supervision for PHI access	Procedures	Implement procedures for authorization and/or supervision of workforce members		
14	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Addressable	Procedures to ensure appropriate PHI access	Procedures	Implement procedures to determine that the access of a workforce member to		
15	164.308(a)(3)(ii)(C)	Termination Procedures	Addressable	Procedures to terminate PHI access	Procedures	Implement procedures for termination access to electronic protected health		
16	164.308(a)(4)(i)	**Information Access Management**	-	P&P to authorize access to PHI	P&P	Implement policies and procedures for authorizing access to electronic protected		
17	164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	**Required**	P&P to separate PHI from other operations	P&P	If a health care clearinghouse is part of a larger organization, the clearinghouse must		
18	164.308(a)(4)(ii)(B)	Access Authorization	Addressable	P&P to authorize access to PHI	P&P	Implement policies and procedures for granting access to electronic protected health		
19	164.308(a)(4)(ii)(C)	Access Establishment and Modification	Addressable	P&P to grant access to PHI	P&P	Implement policies and procedures that, based upon the entity's access authorization		
20	164.308(a)(5)(i)	**Security Awareness Training**	-	Training program for workers and managers	Program	Implement a security awareness and training program for all members of its		
21	164.308(a)(5)(ii)(A)	Security Reminders	Addressable	Distribute periodic security updates	Reminders	Periodic security updates.		
22	164.308(a)(5)(ii)(B)	Protection from Malicious Software	Addressable	Procedures to guard against malicious software	Procedures	Procedures for guarding against, detecting, and reporting malicious software.		
23	164.308(a)(5)(ii)(C)	Log-in Monitoring	Addressable	Procedures and monitoring of log-in attempts	Procedures	Procedures for monitoring log-in attempts and reporting discrepancies.		
24	164.308(a)(5)(ii)(D)	Password Management	Addressable	Procedures for password management	Procedures	Procedures for creating, changing, and safeguarding passwords.		
25	164.308(a)(6)(i)	**Security Incident Procedures**	-	P&P to manage security incidents	P&P	Implement policies and procedures to address security incidents.		
26	164.308(a)(6)(ii)	Response and Reporting	**Required**	Mitigate and document security incidents	Measures	Identify and respond to suspected or known security incidents; mitigate, to the extent		
27	164.308(a)(7)(i)	**Contingency Plan**	-	Emergency response P&P	P&P	Establish (and implement as needed) policies and procedures for responding to an		
28	164.308(a)(7)(ii)(A)	Data Backup Plan	**Required**	Data backup planning & procedures	Procedures	Establish and implement procedures to create and maintain retrievable exact copies		
29	164.308(a)(7)(ii)(B)	Disaster Recovery Plan	**Required**	Data recovery planning & procedures	Procedures	Establish (and implement as needed) procedures to restore loss of data.		
30	164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	**Required**	Business continuity procedures	Procedures	Establish (and implement as needed) procedures to enable continuation of critical		
31	164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Addressable	Contingency planning periodic testing procedures	Procedures	Implement procedures for periodic testing and revision of contingency plans.		
32	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Addressable	Prioritize data and system criticality for contingency	Analysis	Assess the relative criticality of specific applications and data in support of other		
33	164.308(a)(8)	**Evaluation**	-	Periodic security evaluation	Evaluation	Perform a periodic technical and nontechnical evaluation, based initially upon the		
34	164.308(b)(1)	**Business Associate Contracts and Other Arrangements**	-	CE implement BACs to ensure safeguards	-	A covered entity, in accordance with § 164.306, may permit a business associate to		
35	164.308(b)(4)	Written Contract	**Required**	Implement compliant BACs	Contracts	Document the satisfactory assurances required by paragraph (b)(1) of this section		
PHYSICAL SAFEGUARDS								
36	164.310(a)(1)	**Facility Access Controls**	-	P&P to limit access to systems and facilities	P&P	Implement policies and procedures to limit physical access to its electronic		
37	164.310(a)(2)(i)	Contingency Operations	Addressable	Procedures to support emergency operations and	Procedures	Establish (and implement as needed) procedures that allow facility access in support		
38	164.310(a)(2)(ii)	Facility Security Plan	Addressable	P&P to safeguard equipment and facilities	P&P	Implement policies and procedures to safeguard the facility and the equipment there		
39	164.310(a)(2)(iii)	Access Control Validation Procedures	Addressable	Facility access procedures for personnel	Procedures	Implement procedures to control and validate a person's access to facilities based on		
40	164.310(a)(2)(iv)	Maintenance Records	Addressable	P&P to document security-related repairs and	P&P	Implement policies and procedures to document repairs and modifications to the		
41	164.310(b)	**Workstation Use**	-	P&P to specify workstation environment & use	P&P	Implement policies and procedures that specify the proper functions to be performed,		
42	164.310(c)	**Workstation Security**	-	Physical safeguards for workstation access	Controls	Implement physical safeguards for all workstations that access electronic protected		
43	164.310(d)(1)	**Device and Media Controls**	-	P&P to govern receipt and removal of hardware and	P&P	Implement policies and procedures that govern the receipt and removal of hardware		
44	164.310(d)(2)(i)	Disposal	**Required**	P&P to manage media and equipment disposal	P&P	Implement policies and procedures to address the final disposition of electronic		
45	164.310(d)(2)(ii)	Media Re-use	**Required**	P&P to remove PHI from media and equipment	P&P	Implement procedures for removal of electronic protected health information from		
46	164.310(d)(2)(iii)	Accountability	Addressable	Document hardware and media movement	Documentation	Maintain a record of the movements of hardware and electronic media and any		
47	164.310(d)(2)(iv)	Data Backup and Storage	Addressable	Backup PHI before moving equipment	Procedures	Create a retrievable, exact copy of electronic protected health information, when		
TECHNICAL SAFEGUARDS								
48	164.312(a)(1)	**Access Control**	-	Technical (administrative) P&P to manage PHI access	P&P	Implement technical policies and procedures for electronic information systems that		
49	164.312(a)(2)(i)	Unique User Identification	**Required**	Assign unique IDs to support tracking	Procedures	Assign a unique name and/or number for identifying and tracking user identity.		
50	164.312(a)(2)(ii)	Emergency Access Procedure	**Required**	Procedures to support emergency access	Procedures	Establish (and implement as needed) procedures for obtaining necessary electronic		
51	164.312(a)(2)(iii)	Automatic Logoff	Addressable	Session termination mechanisms	Mechanism	Implement electronic procedures that terminate an electronic session after a		
52	164.312(a)(2)(iv)	Encryption and Decryption	Addressable	Mechanism for encryption of stored PHI	Mechanism	Implement a mechanism to encrypt and decrypt electronic protected health		

53	164.312(b)	**Audit Controls**	-	Procedures and mechanisms for monitoring system	Controls	Implement hardware, software, and/or procedural mechanisms that record and		
54	164.312(c)(1)	**Integrity**	-	P&P to safeguard PHI unauthorized alteration	P&P	Implement policies and procedures to protect electronic protected health information		
55	164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health	Addressable	Mechanisms to corroborate PHI not altered	Mechanism	Implement electronic mechanisms to corroborate that electronic protected health		
56	164.312(d)	**Person or Entity Authentication**	-	Procedures to verify identities	Procedures	Implement procedures to verify that a person or entity seeking access to electronic		
57	164.312(e)(1)	**Transmission Security**	-	Measures to guard against unauthorized access to	Controls	Implement technical security measures to guard against unauthorized access to		
56	164.312(e)(2)(i)	Integrity Controls	Addressable	Measures to ensure integrity of PHI on transmission	Controls	Implement security measures to ensure that electronically transmitted electronic		
55	164.312(e)(2)(ii)	Encryption	Addressable	Mechanism for encryption of transmitted PHI	Mechanism	Implement a mechanism to encrypt electronic protected health information whenever		
ORGANIZATIONAL REQUIREMENTS								
56	164.314(a)(1)	**Business Associate Contracts or Other Arrangements**	-	CE must ensure BA safeguards PHI	Process	(i) The contract or other arrangement between the covered entity and its business		
57	164.314(a)(2)	Business Associate Contracts	**Required**	BACs must contain security language	Contracts	(i) Business associate contracts. The contract between a covered entity and a		
58	164.314(b)(1)	**Requirements for Group Health Plans**	-	Plan documents must reflect security safeguards	Plan Doc	Except when the only electronic protected health information disclosed to a plan		
59	164.314(b)(2)(i)	Implement Safeguards	**Required**	Plan sponsor to implement safeguards as appropriate	P&P	The plan documents of the group health plan must be amended to incorporate		
60	164.314(b)(2)(ii)	Ensure Adequate Separation	**Required**	Security measures to separate PHI from plan sponsor	P&P	Ensure that the adequate separation required by		
61	164.314(b)(2)(iii)	Ensure Agents Safeguard	**Required**	Ensure subcontractors safeguard PHI	Contracts	Ensure that any agent, including a subcontractor, to whom it provides this information		
62	164.314(b)(2)(iv)	Report Security Incidents	**Required**	Plan sponsors report breaches to health plan	Process	Report to the group health plan any security incident of which it becomes aware.		
63	164.316(a)	**Policies and Procedures**	-	P&P to ensure safeguards to PHI	P&P	A covered entity must, in accordance with § 164.306: Implement reasonable and		
64	164.316(b)(1)	Documentation	**Required**	Document P&P and actions & activities	Documentation	Documentation.		
65	164.316(b)(2)(i)	Time Limit	**Required**	Retain documentation for 6 years	Procedures	Retain the documentation required by paragraph (b)(1) of this section for 6 years from		
66	164.316(b)(2)(ii)	Availability	**Required**	Documentation available to system administrators	Procedures	Make documentation available to those persons responsible for implementing the		
67	164.316(b)(2)(iii)	Updates	**Required**	Periodic review and updates to changing needs	Process	Review documentation periodically, and update as needed, in response to		

Recommendation



Applicable ISO 17799 Standard(s) & References	HIPAA Citation	Standard Implementation Specification	Implementation	Requirement Description
SECURITY STANDARDS: GENERAL RULES				
12.1.4	164.306(a)	**Ensure Confidentiality, Integrity and Availability**		Ensure CIA and protect against threats
	164.306(b)	**Flexibility of Approach**		Reasonably consider factors in security compliance
12.1.1, 10.1.1	164.306(c)	**Standards**		CEs must comply with standards
	164.306(d)	**Implementation Specifications**		Required and Addressable Implementation Specification requirements
	164.306(e)	**Maintenance**		Ongoing review and modification of security measures
ADMINISTRATIVE SAFEGUARDS				
10.1.1	164.308(a)(1)(i)	**Security Management Process**		P&P to manage security violations
7.1.5, 10.3.1, 10.2.3, 11.1.2, 9.4.1, 9.4.2, 3.1.2, 5.1.1, 6.3.4, 8.2.1, 9.4.3, 9.4.3, 9.4.5, 9.4.6, 9.4.7, 9.4.8, 9.4.9, 9.6.2, 10.1.1, 10.4.3	**164.308(a)(1)(ii)(A)**	**Risk Analysis**	**Required**	**Conduct vulnerability assessment**
6.3.4, 8.1.1, 4.1.2, 3.1.1, 3.1.2, 4.1.1, 5.1.1, 8.1.4, 8.2.1, 8.5.1, 8.6.4, 9.4.4-9.4.9, 9.6.2, 9.7.1, 10.1.1, 11.1.1, 10.4.3, 12.2.2, 12.1.9	**164.308(a)(1)(ii)(B)**	**Risk Management**	**Required**	**Implement security measures to reduce risk of security breaches**
6.3.5,11.1.2	**164.308(a)(1)(ii)(C)**	**Sanction Policy**	**Required**	**Worker sanction for P&P violations**
6.3.5, 9.7.1, 9.7.2, 12.2.1, 12.2.2, 12.3.1, 12.3.2, 6.3.4, 8.1.1, 8.2.2, 10.4.3, 10.5.4, 10.3.4, 10.5.1-10.5.5, 12.2.1, 12.1.5,12.2.2	**164.308(a)(1)(ii)(D)**	**Information System Activity Review**	**Required**	**Procedures to review system activity**
3.1.2, 4.1.3, 4.1.5, 4.1.1, 4.1.2	164.308(a)(2)	**Assigned Security Responsibility**		Identify security official responsible for P&P
9.6.1	164.308(a)(3)(i)	**Workforce Security**		Implement P&P to ensure appropriate PHI access
8.1.4, 9.2.1, 9.2.2, 9.4.2, 9.8.2, 10.4.3	164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Addressable	Authorization/supervision for PHI access
6.1.2, 6.1.4	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Addressable	Procedures to ensure appropriate PHI access
6.1.2, 6.1.4	164.308(a)(3)(ii)(C)	Termination Procedures	Addressable	Procedures to terminate PHI access
9.6.1, 9.5.3, 9.2.2, 10.4.3	164.308(a)(4)(i)	**Information Access Management**		P&P to authorize access to PHI
4.2.1	**164.308(a)(4)(ii)(A)**	**Isolation Health Clearinghouse Functions**	**Required**	**P&P to separate PHI from other operations**
9.1.1, 9.2.2, 9.4.1, 9.6.2, 9.2.1, 8.1.4, 5.2.1	164.308(a)(4)(ii)(B)	Access Authorization		P&P to authorize access to PHI
8.1.4, 9.1.1, 9.2.2, 9.2.4, 9.4.1, 9.5.2, 9.5.3, 9.6.2, 8.6.4, 5.2.1, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 12.1.5	164.308(a)(4)(ii)(C)	Access Establishment and Modification	Addressable	P&P to grant access to PHI
6.2.1, 8.7.7, 9.2.1, 9.2.2, 9.3.2, 9.8.1, 8.7.7, 8.7.4, 12.1.5, 6.1.1, 6.1.3	164.308(a)(5)(i)	**Security Awareness Training**		Training program for workers and managers
6.2.1, 9.3.2, 6.1.1, 6.1.3	164.308(a)(5)(ii)(A)	Security Reminders	Addressable	Distribute periodic security updates
8.3.1, 8.7.4, 4.1.4, 10.4.1, 10.4.2, 10.5.1-10.5.5	164.308(a)(5)(ii)(B)	Protection from Malicious Software	Addressable	Procedures to guard against malicious software
8.4.2, 9.7.1, 9.7.2, 8.4.3	164.308(a)(5)(ii)(C)	Log-in Monitoring	Addressable	Procedures and monitoring of log-in attempts
9.2.3, 9.3.1, 9.5.4	164.308(a)(5)(ii)(D)	Password Management	Addressable	Procedures for password management
8.1.3, 4.1.6	164.308(a)(6)(i)	**Security Incident Procedures**		P&P to manage security incidents
6.3.1,6.3.2,6.3.4,8.1.3	**164.308(a)(6)(ii)**	**Response and Reporting**	**Required**	**Mitigate and document security incidents**
11.1.1, 8.6.3, 4.1.6, 8.1.2	164.308(a)(7)(i)	**Contingency Plan**		Emergency response P&P
8.1.1, 8.4.1, 11.1.3, 11.1.2, 8.6.3	**164.308(a)(7)(ii)(A)**	**Data Backup Plan**	**Required**	**Data backup planning & procedures**
11.1.3	**164.308(a)(7)(ii)(B)**	**Disaster Recovery Plan**	**Required**	**Data recovery planning & procedures**
11.1.3	**164.308(a)(7)(ii)(C)**	**Emergency Mode Operation Plan**	**Required**	**Business continuity procedures**
7.2.2, 11.1.3, 11.1.5, 8.1.5, 7.2.3, 10.5.1-10.5.5	164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Addressable	Contingency planning periodic testing procedures
11.1.2, 11.1.4, 8.1.5, 5.2.2, 8.1.2	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Addressable	Prioritize data and system criticality for contingency planning

4.1.5, 9.7.2, 12.2.1, 12.2.2, 3.1.2, 6.3.4, 8.1.1, 8.2.2	164.308(a)(8)	**Evaluation**		Periodic security evaluation
4.2.1, 4.2.2, 4.3.1, 8.1.6, 12.1.1, 4.1.6, 8.2.1, 8.7.4	164.308(b)(1)	**Business Associate Contracts and Other Arrangements**		CE implement BACs to ensure safeguards
8.71,4.3.1,12.1.1	**164.308(b)(4)**	**Written Contract**	**Required**	**Implement compliant BACs**
PHYSICAL SAFEGUARDS				
7.1.1-7.1.5, 12.1.3, 9.3.2	164.310 (a)(1)	**Facility Access Controls**		P&P to limit access to systems and facilities
7.2.2, 11.1.1, 11.1.3, 12.1.3, 4.1.7, 7.2.3, 7.2.4, 8.1.1	164.310(a)(2)(i)	Contingency Operations	Addressable	Procedures to support emergency operations and recovery
7.1.1, 7.1.3	164.310(a)(2)(ii)	Facility Security Plan	Addressable	P&P to safeguard equipment and facilities
7.1.2, 7.1.4, 9.1.1	164.310(a)(2)(iii)	Access Control Validation Procedures	Addressable	Facility access procedures for personnel
7.2.4, 12.1.3	164.310(a)(2)(iv)	Maintenance Records	Addressable	P&P to document security-related repairs and modifications
2.2.4, 7.2.1, 8.6.1, 7.1.4, 7.2.4, 8.6.1, 12.1.5, 9.3.2, 8.1.5, 4.1.4, 5.2.1	164.310(b)	**Workstation Use**		P&P to specify workstation environment & use
7.2.1, 7.2.4, 8.6.2, 9.3.2, 7.3.2	164.310(c)	**Workstation Security**		Physical safeguards for workstation access
5.1.1, 7.2.5, 7.3.2, 8.7.2, 8.6.7, 9.8.1, 8.5.1, 6.3.3	164.310(d)(1)	**Device and Media Controls**		P&P to govern receipt and removal of hardware and media
7.2.6, 8.6.2	**164.310(d)(2)(i)**	**Disposal**	**Required**	**P&P to manage media and equipment disposal**
7.2.6, 8.6.2	**164.310(d)(2)(ii)**	**Media Re-use**	**Required**	**P&P to remove PHI from media and equipment**
5.1.1, 7.3.2, 7.2.5, 8.7.2, 9.8.1	164.310(d)(2)(iii)	Accountability	Addressable	Document hardware and media movement
8.1.1, 8.4.1, 8.6.3, 12.1.3	164.310(d)(2)(iv)	Data Backup and Storage	Addressable	Backup PHI before moving equipment
TECHNICAL SAFEGUARDS				
9.1.1, 9.4.1, 9.6.1, 12.1.3	164.312(a)(1)	**Access Control**		Technical (administrative) P&P to manage PHI access
9.2.1, 9.2.2	164.312(a)(2)(i)	Unique User Identification	**Required**	Assign unique IDs to support tracking
11.1.3	164.312(a)(2)(ii)	Emergency Access Procedure	**Required**	Procedures to support emergency access
9.5.7, 9.5.8, 7.3.1	164.312(a)(2)(iii)	Automatic Logoff	Addressable	Session termination mechanisms
8.5.1, 8.7.4, 10.3.1, 10.3.2, 10.3.3, 12.1.6	164.312(a)(2)(iv)	Encryption and Decryption	Addressable	Mechanism for encryption of stored PHI
8.1.3, 8.6.2, 9.7.1, 9.7.2, 12.3.1, 12.3.2, 10.3.4, 9.7.3, 4.1.6, 4.1.7	164.312(b)	**Audit Controls**		Procedures and mechanisms for monitoring system activity
12.1.3, 10.2.1, 10.4.2	164.312(c)(1)	**Integrity**		P&P to safeguard PHI unauthorized alteration
10.2.3, 8.1.6	164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information	Addressable	Mechanisms to corroborate PHI not altered
9.4.3, 9.5.3, 8.76, 4.2.1, 9.2.1, 9.2.2, 10.2.1, 10.3.3	164.312(d)	**Person or Entity Authentication**		Procedures to verify identities
10.3.1, 10.3.4, 10.2.4, 4.2.1	164.312(e)(1)	**Transmission Security**		Measures to guard against unauthorized access to transmitted PHI
12.1.3, 10.3.4, 8.7.4, 7.2.3, 8.7.6, 9.4.3, 9.4.3-9.4.9, 9.6.2,10.2.2, 10.2.4, 10.4.3	164.312(e)(2)(i)	Integrity Controls	Addressable	Measures to ensure integrity of PHI on transmission
8.5.1, 8.7.4, 10.3.1, 10.3.2, 10.3.3, 10.4.2, 12.1.6	164.312(e)(2)(ii)	Encryption	Addressable	Mechanism for encryption of transmitted PHI
ORGANIZATIONAL REQUIREMENTS				
4.2.2, 4.3.1, 8.1.6, 12.1.1, 4.2.1, 8.2.1, 4.1.6	164.314(a)(1)	**Business Associate Contracts or Other Arrangements**		CE must ensure BA safeguards PHI
4.2.2, 4.3.1, 8.1.6, 8.7.1, 12.1.1, 8.7.4	164.314(a)(2)	Business Associate Contracts		BACs must contain security language
N/A	**164.314(b)(1)**	**Requirements for Group Health Plans**		**Plan documents must reflect security safeguards**
N/A	**164.314(b)(2)(i)**	**Implement Safeguards**		**Plan sponsor to implement safeguards as appropriate**
N/A	**164.314(b)(2)(ii)**	**Ensure Adequate Separation**		**Security measures to separate PHI from plan sponsor and plan**
N/A	**164.314(b)(2)(iii)**	**Ensure Agents Safeguard**		**Ensure subcontractors safeguard PHI**

N/A	164.314(b)(2)(iv)	Report Security Incidents		Plan sponsors report breaches to health plan
3.1.1, 8.1.1, 12.1.4 (Privacy 6.1.3, 7.3.1, 8.7.4, 8.7.7), 12.1.1, 9.8.2, 12.1.2, 12.2.1, 12.1.4	164.316(a)	**Policies and Procedures**		P&P to ensure safeguards to PHI
8.1.1, 12.1.1, 12.2.1	164.316(b)(1)	Documentation		Document P&P and actions & activities
	164.316(b)(2)(i)	Time Limit		Retain documentation for 6 years
	164.316(b)(2)(ii)	Availability		Documentation available to system administrators
4.1.7, 12.1.1	164.316(b)(2)(iii)	Updates		Periodic review and updates to changing needs