

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Terms & Def	2.1	02	20	022001	Terms and Definitions >> Risk Assessment	164.304	304				
Terms & Def	2.2	02	20	022002	Terms and Definitions > > Risk Assessment	164.308(a)(1)(ii)(A)	308	a	1.2	A	
Terms & Def	2.3	02	30	023001	Terms and Definitions >> Risk Management	164.308(a)(1)(ii)(A)	308	a	1.2	A	
Terms & Def	2.3	02	30	023002	Terms and Definitions >> Risk Management	164.308(a)(1)(ii)(B)	308	a	1.2	B	
Sec Policy	3.1.1	03	11	031101	Information >> Information Security Policy Document	164.316(a)	316	a			
Sec Policy	3.1.1	03	11	031102	Information >> Information Security Policy Document	164.316(b)	316	b			
Sec Policy	3.1.2	03	12	031201	Information >> Review and Evaluation	164.306(e)	306	e			
Sec Policy	3.1.2	03	12	031202	Information >> Review and Evaluation	164.308(a)(8)	308	a	8.0		
Sec Policy	3.1.2	03	12	031203	Information >> Review and Evaluation	164.316(b)(2)(iii)	316	b	2.0	iii	
Org Security	4.1.1	04	11	041101	Information Security Infrastructure >> Management Information Security Forum	164.308(a)(2)	308	a	2.0		
Org Security	4.1.2	04	12	041201	Information Security Infrastructure >> Information Security Co-ordination	164.308(a)(2)	308	a	2.0		
Org Security	4.1.3	04	13	041301	Information Security Infrastructure >> Allocation of Information Security Responsibilities	164.308(a)(2)	308	a	2.0		
Org Security	4.1.4	04	14	041401	Information Security Infrastructure >> Authorization Process for Information Processing Facilities	164.308(a)(1)(I)(B)	308	a	1.1	B	
Org Security	4.1.5	04	15	041501	Information Security Infrastructure >> Specialist Information Security Advice						
Org Security	4.1.6	04	16	041601	Information Security Infrastructure >> Co-operation Between Organizations						
Org Security	4.1.7	04	17	141701	Information Security Infrastructure >> Independent Review of Information Security	164.308(a)(8)	308	a	8.0		
Org Security	4.2.1	04	21	042101	Security of Third Party Access >> Identification of Risks from Third Party Access	164.308(a)(1)(ii)(A)	308	a	1.3	A	
Org Security	4.2.2	04	22	042201	Security of Third Party Access >> Security Requirements in Third Party Contracts	164.308(b)	308	b			
Org Security	4.2.2	04	22	042202	Security of Third Party Access >> Security Requirements in Third Party Contracts	164.314(a)(1)	314	a	1.0		
Org Security	4.3.1	04	31	043101	Security of Third Party Access >> Security Requirements in Outsourcing Contracts	164.308(b)	308	b			

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Org Security	4.3.1	04	31	043103	Security of Third Party Access >> Security Requirements in Outsourcing Contracts	164.314(a)(1)	314	a	1.0		
Asset Class	5.1.1	05	11	051101	Accountability for Assets >> Inventory of Assets	164.308(a)(7)(ii)(E)	308	a	7.2	E	
Asset Class	5.2.1	05	21	052101	Information Classification >> Classification Guidelines	164.308(a)(7)(ii)(E)	308	a	7.2	E	
Asset Class	5.2.2	05	22	052201	Information Classification >> Information Labeling and Handling	164.308(a)(7)(ii)(E)	308	a	7.2	E	
Personnel	6.1.1	06	11	061101	Security in Job Definition and Resourcing >> Including Security in Job Responsibilities	164.308(a)(3)(i)	308	a	3.1		
Personnel	6.1.2	06	12	061201	Security in Job Definition and Resourcing >> Personnel Screening and Policy	164.308(a)(3)(ii)(B)	308	a	3.2	B	
Personnel	6.1.3	06	13	061302	Security in Job Definition and Resourcing >> Confidentiality Agreements	164.308(a)(3)(i)	308	a	3.1		ISO standard is implied, but not specifically required, in HIPAA
Personnel	6.1.3	06	13	061303	Security in Job Definition and Resourcing >> Confidentiality Agreements	164.314(a)(1)	314	a	1.0		
Personnel	6.1.3				Security	164.308(b)					
Personnel	6.1.4	06	14	061401	Security in Job Definition and Resourcing >> Terms and Conditions of Employment	164.308(a)(1)(ii)(C)	308	a	1.2	C	ISO standard is implied, but not specifically required, in HIPAA
Personnel	6.1.4	06	14	061402	Security in Job Definition and Resourcing >> Terms and Conditions of Employment	164.308(a)(3)(i)	308	a	3.1		ISO standard is implied, but not specifically required, in HIPAA
Personnel	6.2.1	06	21	062101	User Training >> Information Security Education and Training	164.308(a)(5)(i)	308	a	5.1		
Personnel	6.2.1	06	21	062102	User Training >> Information Security Education and Training	164.308(a)(5)(ii)(A)	308	a	5.2	A	
Personnel	6.2.1	06	21	062103	User Training >> Information Security Education and Training	164.308(a)(5)(ii)(B)	308	a	5.2	B	
Personnel	6.3.1	06	31	063102	Responding to Security Incidents and Malfunctions >> Reporting Security Incidents	164.308(a)(6)	308	a	6.2		

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Personnel	6.3.2	06	32	063201	Responding to Security Incidents and Malfunctions >> Reporting Security Weaknesses	164.308(a)(1)(ii)(D)	308	a	1.2	D	ISO standard is implied, but not specifically required, in HIPAA - of course in order to have incident reports someone must report, but HIPAA does not require all users of information services to report "any observed or suspected security weaknesses"
Personnel	6.3.2	06	32	063202	Responding to Security Incidents and Malfunctions >> Reporting Security Weaknesses	164.308(a)(6)(ii)	308	a	6.2		ISO standard is implied, but not specifically required, in HIPAA - of course in order to have incident reports someone must report, but HIPAA does not require all users of information services to report "any observed or suspected security weaknesses"
Personnel	6.3.4	06	34	063401	Responding to Security Incidents and Malfunctions >> Learning from Incidents	164.308(a)(6)(ii)					
Personnel	6.3.4					164.308(a)(1)(ii)(B)					

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Personnel	6.3.5	06	35	063501	Responding to Security Incidents and Malfunctions >> Disciplinary Process	164.308(a)(1)(ii)(C)	308	a	1.2	C	
Physical	7.1.1	07	11	071101	Secure Areas >> Physical Security Perimeter	164.310(a)(1)	310	a	1.0		
Physical	7.1.1	07	11	071102	Secure Areas >> Physical Security Perimeter	164.310(a)(2)(ii)	310	a	2.2		
Physical	7.1.2	07	12	071201	Secure Areas >> Physical Entry Controls	164.310(a)(1)	310	a	1.0		
Physical	7.1.2	07	12	071202	Secure Areas >> Physical Entry Controls	164.310(a)(2)(ii)	310	a	2.2		
Physical	7.1.2	07	12	071203	Secure Areas >> Physical Entry Controls	164.310(a)(2)(iii)	310	a	2.3		
Physical	7.1.3	07	13	071301	Secure Areas >> Securing Offices, Rooms and Facilities	164.310(a)(1)	310	a	1.0		
Physical	7.1.3	07	13	071302	Secure Areas >> Securing Offices, Rooms and Facilities	164.310(a)(2)(ii)	310	a	2.2		
Physical	7.1.3	07	13	071303	Secure Areas >> Securing Offices, Rooms and Facilities	164.310(a)(2)(iii)	310	a	2.3		
Physical	7.1.3	07	13	071304	Secure Areas >> Securing Offices, Rooms and Facilities	164.310(b)	310	b			
Physical	7.1.3	07	13	071305	Secure Areas >> Securing Offices, Rooms and Facilities	164.310(c)	310	c			
Physical	7.1.4	07	14	071401	Secure Areas >> Working in Secure Areas	164.310(a)(1)	310	a	1.0		
Physical	7.1.4	07	14	071402	Secure Areas >> Working in Secure Areas	164.310(a)(2)(ii)	310	a	2.2		
Physical	7.1.4	07	14	071403	Secure Areas >> Working in Secure Areas	164.310(a)(2)(iii)	310	a	2.3		
Physical	7.1.4	07	14	071404	Secure Areas >> Working in Secure Areas	164.310(b)	310	b			
Physical	7.1.4	07	14	071405	Secure Areas >> Working in Secure Areas	164.310(c)	310	c			
Physical	7.1.5	07	15	071501	Secure Areas >> Isolated Delivery and Loading Areas	164.310(a)(1)	310	a	1.0		
Physical	7.1.5	07	15	071502	Secure Areas >> Isolated Delivery and Loading Areas	164.310(a)(2)(ii)	310	a	2.2		
Physical	7.1.5	07	15	071503	Secure Areas >> Isolated Delivery and Loading Areas	164.310(a)(2)(iii)	310	a	2.3		
Physical	7.2.1	07	21	072101	Equipment Security >> Equipment Sitting and Protection	164.310(a)(2)(ii)	310	a	2.2		

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Physical	7.2.1	07	22	072201	Equipment Security >> Equipment Siting and Protection	164.310(c)	310	c			Requires a very broad definition of "workstation" in HIPAA, i.e., ISO is looking at all kinds of equipment, not just workstations
Physical	7.2.2	07	22	072201	Equipment Security >> Power Supplies	164.310(a)(2)(ii)	310	a	2.2		ISO standard is implied, but not specifically required, in HIPAA
Physical	7.2.3	07	23	072301	Equipment Security >> Cabling Security	164.310(a)(2)(ii)	310	a	2.2		HIPAA deals generally with "access, tampering and theft;" this ISO section deals protecting telecommunication cable from damage or tampering
Physical	7.2.4	07	24	072401	Equipment Security >> Equipment Maintenance	164.310(a)(2)(ii)	310	a	2.2		
Physical	7.2.4	07	24	072402	Equipment Security >> Equipment Maintenance	164.310(a)(2)(iii)					
Physical	7.2.4	07	24	072402	Equipment Security >> Equipment Maintenance	164.310(a)(1)					
Physical	7.2.4	07	24	072402	Equipment Security >> Equipment Maintenance	164.310(d)(2)(iii)					
Physical	7.2.4	07	24	072402	Equipment Security >> Equipment Maintenance	164.310(d)(2)(iv)					
Physical	7.2.5	07	25	072501	Equipment Security >> Security of Equipment Off-Premises	164.310(a)(2)(ii)	310	a	2.2		
Physical	7.2.5	07	25	072502	Equipment Security >> Security of Equipment Off-Premises	164.310(d)(2)(iii)	310	d	2.3		
Physical	7.2.6	07	26	072601	Equipment Security >> Secure Disposal or Re-Use of Equipment	164.310(a)(2)(ii)	310	a	2.2		This element could be a standard for all requirements under physical security

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Physical	7.2.6	07	26	072602	Equipment Security >> Secure Disposal or Re-Use of Equipment	164.310(d)(2)	310	d	2.0		
Physical	7.3.1	07	31	073101	General Controls >> Clear Desk and Clear Screen Policy	164.310(b)	310	b			
Physical	7.3.1	07	31	073102	General Controls >> Clear Desk and Clear Screen Policy	164.310(c)	310	c			
Physical	7.3.2	07	32	073201	General Controls >> Removal of Property	164.310(d)(2)(iii)	310	d	2.3		
Comm & Ops	8.1.1	08	11	081101	Operational Procedures and Responsibilities >> Documented Operating Procedures						
Comm & Ops	8.1.2	08	12	081201	Operational Procedures and Responsibilities >> Operational Change Control						
Comm & Ops	8.1.3	08	13	081301	Operational Procedures and Responsibilities >> Incident Management Procedures	164.308(a)(6)	308	a	6.0		
Comm & Ops	8.1.4	08	14	081401	Operational Procedures and Responsibilities >> Segregation of Duties						
Comm & Ops	8.1.6	08	16	081601	Operational Procedures and Responsibilities >> External Facilities Management	164.308(b)(1)	308	b	1.0		
Comm & Ops	8.1.6	08	16	081601	Operational Procedures and Responsibilities >> External Facilities Management	164.314(a)					
Comm & Ops	8.2.1	08	21	082101	System Planning and Acceptance >> Capacity Planning						
Comm & Ops	8.2.2	08	22	082201	System Planning and Acceptance >> System Acceptance						
Comm & Ops	8.3.1	08	31	083101	Protection Against Malicious Software >> Controls Against Malicious Software	164.308(a)(5)(ii)(B)	308	a	5.2	B	
Comm & Ops	8.3.1	08	31	083101	Protection Against Malicious Software >> Controls Against Malicious Software	164.312(a)(1)					
Comm & Ops	8.4.1	08	41	084101	Housekeeping >> Information Back-Up	164.308(a)(7)(ii)(A)	308	a	7.2	A	
Comm & Ops	8.4.1	08	41	084102	Housekeeping >> Information Back-Up	164.310(d)(2)(iv)	310	d	2.4		
Comm & Ops	8.4.2	08	42	084201	Housekeeping >> Operator Logs	164.308(a)(1)(ii)(D)	308	a	1.2	D	
Comm & Ops	8.4.2	08	42	084201	Housekeeping >> Operator Logs	164.312(b)					
Comm & Ops	8.5.1	08	51	085101	Network Management >> Network Controls	164.312(e)(1)	312	e	1.0		
Comm & Ops	8.5.1	08	51	085101	Network Management >> Network Controls	164.312(a)(1)					
Comm & Ops	8.6.1	08	61	086101	Media Handling and Security >> Management of Removable Computer Media	164.310(d)	310	d	1.0		
Comm & Ops	8.6.2	08	62	086201	Media Handling and Security >> Disposal of Media	164.310(d)(2)(i)	310	d	2.1		

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Comm & Ops	8.6.2	08	62	086201	Media Handling and Security >> Disposal of Media	164.310(d)(2)(iii)					
Comm & Ops	8.6.3	08	63	086301	Media Handling and Security >> Information Handling Procedures	164.312(c)(2)	312	c	2.0		
Comm & Ops	8.6.3	08	63	086301	Media Handling and Security >> Information Handling Procedures	164.310(d)(1)					
Comm & Ops	8.6.3	08	63	086301	Media Handling and Security >> Information Handling Procedures	164.310(a)					
Comm & Ops	8.6.3	08	63	086301	Media Handling and Security >> Information Handling Procedures	164.310(a)(2)(iii)					
Comm & Ops	8.6.3	08	63	086301	Media Handling and Security >> Information Handling Procedures	164.310(d)(2)(iii)					
Comm & Ops	8.6.4	08	64	086401	Media Handling and Security >> Security of System Documentation						
Comm & Ops	8.7.1	08	71	087101	Exchanges of Information and Software >> Information and Software Exchange Agreements	164.308(b)(1)	308	b	1.0		
Comm & Ops	8.7.2	08	72	087201	Exchanges of Information and Software >> Security of Media in Transit	164.310(d)(1)	310	d	1.0		ISO is very specific here, and should be used as GUIDANCE ONLY
Comm & Ops	8.7.3	08	73	087302	Exchanges of Information and Software >> Electronic Commerce Security	164.312(e)	312	e			
Comm & Ops	8.7.4	08	74	087402	Exchanges of Information and Software >> Security of Electronic Mail	164.312(a)(1)					
Comm & Ops	8.7.4	08	74	087402	Exchanges of Information and Software >> Security of Electronic Mail	164.312(e)(1)	312	e	1.0		
Comm & Ops	8.7.5	08	75	087501	Exchanges of Information and Software >> Security of Electronic Office Systems	164.310(b);	310	b			
Comm & Ops	8.7.5	08	75	087501	Exchanges of Information and Software >> Security of Electronic Office Systems	164.310 (a)(1)					
Comm & Ops	8.7.5	08	75	087501	Exchanges of Information and Software >> Security of Electronic Office Systems	164.312(a)(1)					
Comm & Ops	8.7.6	08	76	087601	Exchanges of Information and Software >> Publicly Available Systems	164.312(a)(1)					
Comm & Ops	8.7.6	08	76	087601	Exchanges of Information and Software >> Publicly Available Systems	164.312(c)					
Comm & Ops	8.7.6	08	76	087601	Exchanges of Information and Software >> Publicly Available Systems	164.312(d)					
Comm & Ops	8.7.6	08	76	087601	Exchanges of Information and Software >> Publicly Available Systems	164.312(e)					
Access Control	9.1.1	09	11	091101	Business Requirements for Access Control Policy	164.308(a)(3)(i)	308	a	3.1		

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Access Control	9.1.1	09	11	091102	Business Requirements for Access Control Policy	164.312(a)(1)	312	a	1.0		
Access Control	9.2.1	09	21	092101	User Access Management >> User Registration	164.308(a)(4)(i)	308	a	4.1		
Access Control	9.2.1	09	21	092102	User Access Management >> User Registration	164.308(a)(3)(ii)(C)	308	a	3.2	C	
Access Control	9.2.1	09	21	092103	User Access Management >> User Registration	164.308(a)(4)(ii)(B)	308	a	4.2	B	
Access Control	9.2.1	09	21	092104	User Access Management >> User Registration	164.308(a)(4)(ii)(C)	308	a	4.2	C	
Access Control	9.2.1	09	21	092105	User Access Management >> User Registration	164.312(a)(2)(I)					This does include non technical matters
Access Control	9.2.2	09	22	092201	User Access Management >> Privilege Management	164.308(a)(4)(i)	308	a	4.1		
Access Control	9.2.2	09	22	092203	User Access Management >> Privilege Management	164.308(a)(4)(ii)(B)	308	a	4.2	B	
Access Control	9.2.2	09	22	092204	User Access Management >> Privilege Management	164.308(a)(4)(ii)(C)	308	a	4.2	C	
Access Control	9.2.2	09	22	092205	User Access Management >> Privilege Management	164.312(a)(1)	312	a	1.0		
Access Control	9.2.3	09	23	092304	User Access Management >> User Password Management	164.308(a)(5)(ii)(D)					User password management is a training implementation specification in HIPAA
Access Control	9.2.4	09	24	092402	User Access Management >> Review of User Access Rights	164.308(a)(4)(ii)(C)	308	a	4.2	C	
Access Control	9.3.1	09	31	093101	User Responsibilities >> Password Use	164.308(a)(5)(ii)(D);	308	a	5.2	D	Implied in HIPAA
Access Control	9.3.2	09	32	093201	User Responsibilities >> Unattended User Equipment	164.310(b)	310	b			
Access Control	9.3.2	09	32	093202	User Responsibilities >> Unattended User Equipment	164.310(c)	310	c			
Access Control	9.3.2	09	32	093203	User Responsibilities >> Unattended User Equipment	164.312(a)(2)(iii)	312	a	2.3		
Access Control	9.4.1	09	41	094101	Network Policy on Use of Network Services	164.312(a)(1)	312	a	1.0		
Access Control	9.4.1	09	41	094103	Network Policy on Use of Network Services	164.312(d)(2)	312	d	2.0		
Access Control	9.4.1	09	41	094103	Network Policy on Use of Network Services	164.308(a)(4)(ii)(B)					
Access Control	9.4.3	09	43	094302	Network User Authentication for External Connections	164.312(d)	312	d			

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Access Control	9.4.4	09	44	094401	Network Node Authentication	164.312(d)	312	d			
Access Control	9.4.5	09	45	094501	Network Remote Diagnostic Port Protection	164.312(a)(2)(i)	312	1	2.2		
Access Control	9.4.5	09	45	094501	Network Remote Diagnostic Port Protection	164.312(a)(1)					
Access Control	9.4.5	09	45	094502	Network Remote Diagnostic Port Protection	164.312(d)	312	d			
Access Control	9.4.7	09	47	094702	Network Network Connection Control	164.312(e)(1)	312	e	1.0		
Access Control	9.4.7	09	47	094702	Network Network Connection Control	164.312(e)(1)	312	e	1.0		
Access Control	9.4.8	09	48	094802	Network Network Routing Control	164.312(a)(1)	312	a	1.0		
Access Control	9.5.2	09	52	095202	Operating System Terminal Log-On Procedures	164.308(a)(5)(ii)(C)	308	a	5.2	C	ISO standard is implied, but not specifically required, in HIPAA
Access Control	9.5.3	09	53	095302	Operating System User Identification and Authentication	164.312(a)(2)(i)	312	a	2.1		
Access Control	9.5.4	09	54	095401	Operating System Password Management System	164.308(a)(5)(ii)(D)	308	a	5.2	D	ISO standard is implied, but not specifically required, in HIPAA
Access Control	9.5.6	09	56	095601	Operating System Duress Alarm to Safeguard Users						
Access Control	9.5.7	09	57	095702	Operating System Terminal Time-Out	164.312(a)(2)(iii)	312	a	2.3		
Access Control	9.5.8	09	58	095802	Operating System Limitation of Connection Time	164.312(a)(2)(iii)	312	a	2.3		
Access Control	9.6.1	09	61	096101	Application Information Access Restriction	164.312(a)(1)	312	a	1.0		
Access Control	9.6.1	09	61	096101	Application Information Access Restriction	164.308(a)(4)(ii)(B)	308	a	4.2	B	
Access Control	9.6.1	09	61	096101	Application Information Access Restriction	164.308.(a)(4)(ii)(C)	308	a	4.2	C	
Access Control	9.6.2	09	62	096201		164.312(a)(1)					Not specifically required by HIPAA, but could be guidance under certain circumstances
Access Control	9.7.1	09	71	097101	Monitoring System Access and Use >> Event Logging	164.312(b)	312	b			
Access Control	9.7.2	09	72	097201	Monitoring System Access and Use >> Monitoring System Use	164.308(a)(1)(ii)(D)	308	a	1.2	D	

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Access Control	9.7.2	09	72	097202	Monitoring System Access and Use >> Monitoring System Use	164.308(a)(5)(ii)(C)	308	a	5.2	C	ISO standard is implied, but not specifically required, in HIPAA
Access Control	9.7.3	09	73	097301	Monitoring System Access and Use >> Clock Synchronization						
Access Control	9.8.1	09	81	098101	Mobile Computing and Teleworking >> Mobile Computing	164.312(a)(1)	312	a	1.0		ISO is so general it implicates many HIPAA topics
Access Control	9.8.1	09	81	098101	Mobile Computing and Teleworking >> Mobile Computing	164.308(a)(1)(i)	308	a	1.1		
Access Control	9.8.1	09	81	098101	Mobile Computing and Teleworking >> Mobile Computing	164.308(a)(5)(i)	308	a	5.1		
Access Control	9.8.1	09	81	098101	Mobile Computing and Teleworking >> Mobile Computing	164.310(b)	310	b			HIPAA does not distinguish between Mobile, Teleworking, and other sites, everything focuses on data and not the location of the user
Access Control	9.8.1	09	81	098101	Mobile Computing and Teleworking >> Mobile Computing	164.310(c)	310	c			
Access Control	9.8.1	09	81	098101	Mobile Computing and Teleworking >> Mobile Computing	164.312((e)(1)	312	e	1.0		
Access Control	9.8.2	09	82	098201	Mobile Computing and Teleworking >> Teleworking	164.312(a)(1)	312	a	1.0		
Access Control	9.8.2					See Comments					Everything in 9.8.1 equally applies in 9.8.2
Sys Dev	10.1.1	10	11	101101	Security Requirements of Systems >> Security Requirements Analysis and Specifications	164.308(a)(1)(i)	308	a	1.1		
Sys Dev	10.1.1	10	12	101101	Security Requirements of Systems >> Security Requirements Analysis and Specifications	164.308(a)(1)(ii)(C)	308	a	1.2	C	
Sys Dev	10.1.1	10	11	101101	Security Requirements of Systems >> Security Requirements Analysis and Specifications	164.308(a)(1)(ii)(B)	308	a	1.2	B	

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Sys Dev	10.2.2	10	22	102201	Security in Application Systems >> Control of Internal Processing	164.312(c)(1)	312	c	1.0		
Sys Dev	10.2.3	10	23	102301	Security in Application Systems >> Message Authentication	164.312(c)(1)	312	c	1.0		
Sys Dev	10.2.3	10	23	102302	Security in Application Systems >> Message Authentication	164.312(d)(2)	312	d	2.0		
Sys Dev	10.2.3	10	23	102303	Security in Application Systems >> Message Authentication	164.312(e)(2)	312	e	2.0		
Sys Dev	10.2.4	10	24	102401	Security in Application Systems >> Output Data Validation	164.312(c)(2)					
Sys Dev	10.3.1	10	31	103101	Cryptographic Controls >> Policy on the Use of Cryptographic Controls	164.308(a)(1)(i)	308	a	1.1		
Sys Dev	10.3.1	10	31	103102	Cryptographic Controls >> Policy on the Use of Cryptographic Controls	164.308(a)(1)(ii)(A)	308	a	1.2	A	
Sys Dev	10.3.2	10	32	103201	Cryptographic Controls >> Encryption	164.312(a)(2)(iv)	312	a	2.4		
Sys Dev	10.3.2	10	32	103202	Cryptographic Controls >> Encryption	164.312(e)(2)(ii)	312	e	2.2		
Sys Dev	10.3.3	10	33	103303	Cryptographic Controls >> Digital Signatures	164.312(c)(1)	312	c	1.0		No specific requirement for digital signatures in final regulations. Digital signatures are mentioned in preamble but are not specific to encryption
Sys Dev	10.3.4	10	34	103401	Cryptographic Controls >> Non Repudiation Services	164.312(c)(1)	312	c	1.0		
Sys Dev	10.3.5	10	35	103501	Cryptographic Controls >> Key Management	164.312(a)(2)(iv)	312	a	2.2		Not specifically required by HIPAA, but ISO provides guidance when encryption is needed

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Sys Dev	10.4.1	10	41	104101	Security of System Files >> Control of Operational Software	164.312(c)(1)	312	c	1.0		ISO applies to underlying software architecture, not data, not specifically required by HIPAA but serves as guidance where needed
Sys Dev	10.4.2	10	42	104201	Security of System Files >> Protection of System Test Data	164.312(c)(1)	312	c	1.0		Not specifically required by HIPAA, but could be guidance under certain circumstances
Sys Dev	10.4.3	10	43	104301	Security of System Files >> Access Control to Program Source Library	164.312(c)(1)	312	c	1.0		Not specifically required by HIPAA, but could be guidance under certain circumstances
Sys Dev	10.5.1	10	51	105101	Security in Development and Support Processes >> Change Control Procedures	164.312(c)(1)	312	c	1.0		Not specifically required by HIPAA, but could be guidance under certain circumstances
Sys Dev	10.5.2	10	52	105201	Security in Development and Support Processes >> Technical Review of Operating System Changes	164.312(c)(1)	312	c	1.0		Not specifically required by HIPAA, but could be guidance under certain circumstances
Sys Dev	10.5.3	10	53	105301	Security in Development and Support Processes >> Restrictions on Changes to Software Packages	164.312(c)(1)	312	c	1.0		Not specifically required by HIPAA, but could be guidance under certain circumstances

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Sys Dev	10.5.4	10	54	105401	Security in Development and Support Processes >> Covert Channels and Trojan Code	164.308(a)(5)(ii)(B)	308	a	5.2	B	
Sys Dev	10.5.4	10	54	105402	Security in Development and Support Processes >> Covert Channels and Trojan Code	164.312(c)(1)	312	c	1.0		
Sys Dev	10.5.5	10	55	105501	Security in Development and Support Processes >> Outsourced Software Development	164.312(c)(1)	312	e	1.0		
Continuity	11.1.1	11	11	111101	Aspects of Business Continuity Management Process	164.308(a)(7)(i)	308	a	7.1		
Continuity	11.1.1	11	11	111102	Aspects of Business Continuity Management Process	164.310(a)(2)(i)	310	a	2.1		
Continuity	11.1.1	11	11	111103	Aspect of Business Continuity Management Process	164.312(a)(2)(ii)	312	a	2.2		
Continuity	11.1.2	11	12	111201	Aspects of Business Continuity and Impact Analysis	164.308(a)(7)(ii)(E)	308	a	7.2	E	
Continuity	11.1.3	11	13	111301	Aspects of Writing and Implementing Continuity Plans	164.308(a)(7)(ii)(A)	308	a	7.2	A	
Continuity	11.1.3	11	13	111302	Aspects of Writing and Implementing Continuity Plans	164.308(a)(7)(ii)(B)	308	a	7.2	B	
Continuity	11.1.3	11	13	111303	Aspects of Writing and Implementing Continuity Plans	164.308(a)(7)(ii)(C)	308	a	7.2	C	
Continuity	11.1.3	11	13	111304	Aspects of Writing and Implementing Continuity Plans	164.308(a)(7)(ii)(D)	308	a	7.2	D	
Continuity	11.1.3	11	13	111305	Aspects of Writing and Implementing Continuity Plans	164.310(a)(2)(i)	310	a	2.1		
Continuity	11.1.3	11	13	111306	Aspects of Writing and Implementing Continuity Plans	164.312(a)(2)(ii)	312	a	2.2		
Continuity	11.1.4	11	14	111401	Aspects of Business Continuity Planning Framework						
Continuity	11.1.5	11	15	111501	Aspects of Testing, Maintenance and Re-Assessing Business Continuity Plans	164.308(a)(7)(ii)(D)	308	a	7.2	D	
Compliance	12.1.1	12	11	121101	Compliance with Legal Requirements >> Identification of Applicable Legislation						
Compliance	12.1.2	12	12	121201	Compliance with Legal Requirements >> Intellectual Property Rights (IPR)						
Compliance	12.1.3	12	13	121301	Compliance with Legal Requirements >> Safeguarding of Organizational Records	164.316(b)(1)	316	b	1.0		Limited to evidence of compliance with the HIPAA Security Rule
Compliance	12.1.4	12	14	121401	Compliance with Legal Requirements >> Data Protection and Privacy of Personal Information	164.306(a)	306	a			

DRAFT Comparison of ISO 17799 and HIPAA Security Rule

ISO Section	ISO #	Sec XX	Sub YY	17799 ID XXYYZZ	ISO 17799:2000 Section Headings	HIPAA Security Rule Cross Reference	Index1	Index2	Index3	Index4	Comments
Compliance	12.1.4	12	14	121402	Compliance with Legal Requirements >> Data Protection and Privacy of Personal Information	164.308(a)(2)	308	a	2.0		
Compliance	12.1.5	12	15	121501	Compliance with Legal Requirements >> Prevention of Misuse of Information Processing Facilities	164.310(a)(1)	310	a	1.0		
Compliance	12.1.5	12	15	121502	Compliance with Legal Requirements >> Prevention of Misuse of Information Processing Facilities	164.310(b)	310	b			
Compliance	12.1.5	12	15	121503	Compliance with Legal Requirements >> Prevention of Misuse of Information Processing Facilities	164.308(a)(3)	308	a	3.0		
Compliance	12.2.1	12	21	122101	Reviews of Security Policy/Technical Compliance with Security Policy	164.308(a)(8)	308	a	8.0		
Compliance	12.2.2	12	22	122201	Reviews of Security Policy/Technical Technical Compliance Checking	164.308(a)(8)	308	a	8.0		
Compliance	12.3.1	12	31	123101	System Audit Considerations >> System Audit Controls	164.308(a)(8)	308	a	8.0		