HITRUST CSF to HIPAA Relationship Matrix v3

Scope

This matrix is provided to reflect changes in CSF 2014 (v6.0), which ensure tighter alignment between the CSF and NIST with respect to the mapping of controls in NIST SP 800-53 R4 to ISO/IEC 27001:2005 clauses and to HIPAA per NIST SP 800-66 R1.

Relationships

The matrix provides "many-to-many" mappings of the relationships between the CSF and the HIPAA Security Rule required and addressable implementation specifications due to differences in their structure as well as the very specific nature of CSF controls as compared to the more general HIPAA specifications. As a result, the matrix indicates two types of mappings: very specific, direct relationships between controls and based on how NIST is mapped to the CSF specifications and their more general, supportive relationships.

For questions, visit our forum on HITRUST Central, Ask HITRUST, at: https://www.hitrustcentral.net/forums/112.aspx.

General: This document is protected with a password. If you would like to make corrections or other modifications, please contact HITRUST. NOTE that you assume the risk, responsibility and potential legal liability for any issues that may arise a should you attempt to unprotect the document and/or make your own changes.

CSF - HIPAA Cross-Reference Matrix v3

HIPAA / CSF	164.308(a)(1)(i) Security Mgmt Process	164.308(a)(1)(ii)(A) Risk Analysis (R)	164.308(a)(1)(ii)(B) Risk Mgmt (R)	164.308(a)(1)(ii)(C) Sanction Policy (R)	164.308(a)(1)(ii)(D) Information System Activity Review (R)	164.308(a)(2) Assigned Security Responsibility	162.308(a)(3)(i) Workforce Security	164.308(a)(3)(ii)(A) Authorization and/ or Supervision (A)	164.308(a)(3)(ii)(B) Workforce Clearance Procedures (A)	164.308(a)(3)(ii)(C) Termination Procedures (A)	164.308(a)(4)(i) Information Access Management	164.308(a)(4)(ii)(A) Isolation Health Clearinghouse Functions (R)	164.308(a)(4)(ii)(B) Access Authorization	164.308(a)(4)(ii)(C) Access Establishment & Modificaiton (A)	164.308(a)(5)(i) Security Awareness Training	164.308(a)(5)(ii)(A) Security Reminders (A)	164.308(a)(5)(ii)(B) Protection from Malicious Software (A)	164.308(a)(5)(ii)(C) Log-in Monitoring (A)
0.a InfoSec Mgmt Program	X	X	X															
01.a Access Control Policy*							X	X			X		X					
01.b User Registration*								X	X		X		X	X				X
01.c Privilege Management							X	X	X		X	X	X	X				X
01.d User Password Management*																		
01.e Review of User Access Rights								X	X		X		X	X				X
01.f Password Use*																		
01.g Unattended User Equipment																		
01.h Clear Desk and Clear Screen Policy*								O			O		O	O				
01.i Policy on Use of Network Services*							X	X			X	O	X	X				
01.j User Auth. for Ext. Connections*																		
01.k Equip Ident. in Networks																		
01.l Remote Diagnostic & Config Port Protection							O				O	O						
01.m Segregation in Networks*								X					X					
01.n Network Connection Control*																		
01.o Network Routing Control*								X					X					
01.p Secure Log-on Procedures																		
01.q User Identification and Authentication*									O		O		O	O				O
01.r Password Mgmt System*																		
01.s Use of System Utilities							X	X			X	X	X	X				O
01.t Session Time-out								O	O		O		O	O				O
01.u Limitation of Connection Time								O	O		O		O	O				O
01.v Information Access Restriction*							X	X			X	X	X	X				
01.w Sensitive System Isolation*																		
01.x Mobile Computing and Communications*							O	O	O		O		O	O				
01.y Teleworking*							O	O	O		O		O	O				
02.a Roles and Responsibilities*	O						O	X	X	X	O		O	O	O			
02.b Screening									X									
02.c Terms and Conditions of Employment								X	X				X					
02.d Management Responsibilities*								X	O				X					
02.e InfoSec Awareness, Education, and Training*															X	X	X	
02.f Disciplinary Process*				X														
02.g Termination or Change Responsibilities										X								
02.h Return of Assets										X								
02.i Removal of Access Rights*								X	X	X	X		X	X				X
03.a Risk Management Program Development	X																	
03.b Performing Risk Assessments*		X	X			X												
03.c Risk Mitigation*																		
03.d Risk Evaluation																		

HIPAA / CSF	164.308(a)(5)(ii)(D) Password Management (A)	164.308(a)(6)(i) Security Incident Procedures	164.308(a)(6)(ii) Response & Reporting (R)	164.308(a)(7)(i) Contingency Plan	164.308(a)(7)(ii)(A) Data Backup Plan (R)	164.308(a)(7)(ii)(B) Disaster Recovery Plan (R)	164.308(a)(7)(ii)(C) Emergency Mode Operation Plan (R)	164.308(a)(7)(ii)(D) Testing & Revisoin Procedures (A)	164.308(a)(7)(ii)(E) Application and Data Criticality Analysis (A)	164.308(a)(8) Evaluation	164.308(b)(1) Business Associate Contracts & Other Arrangements	164.308(b)(4) Written Contract (R)	164.310(a)(1) Facility Access Controls	164.310(a)(2)(i) Contingency Operations (A)	164.310(a)(2)(ii) Facility Security Plan (A)	164.310(a)(2)(iii) Access Control Validation Procedures (A)	164.310(a)(2)(iv) Maintenance Records (A)	164.310(b) Workstation Use
0.a InfoSec Mgmt Program										X								
01.a Access Control Policy*																		
01.b User Registration*	X															O		
01.c Privilege Management																		O
01.d User Password Management*	X																	
01.e Review of User Access Rights																		
01.f Password Use*	X																	
01.g Unattended User Equipment													X					X
01.h Clear Desk and Clear Screen Policy*																		X
01.i Policy on Use of Network Services*																		O
01.j User Auth. for Ext. Connections*											O	O						X
01.k Equip Ident. in Networks																		O
01.l Remote Diagnostic & Config Port Protection																O	O	O
01.m Segregation in Networks*																		X
01.n Network Connection Control*																		X
01.o Network Routing Control*																		X
01.p Secure Log-on Procedures	X																	
01.q User Identification and Authentication*	X																	
01.r Password Mgmt System*	X																	
01.s Use of System Utilities																X		X
01.t Session Time-out																		X
01.u Limitation of Connection Time																		
01.v Information Access Restriction*																X		X
01.w Sensitive System Isolation*																		
01.x Mobile Computing and Communications*																		X
01.y Teleworking*														X				X
02.a Roles and Responsibilities*		O		O						O	O		O		O	O	O	O
02.b Screening																		
02.c Terms and Conditions of Employment																		X
02.d Management Responsibilities*											X	O						O
02.e InfoSec Awareness, Education, and Training*		X						X										
02.f Disciplinary Process*																		
02.g Termination or Change Responsibilities																		
02.h Return of Assets																		
02.i Removal of Access Rights*													O			O		
03.a Risk Management Program Development																		
03.b Performing Risk Assessments*																		
03.c Risk Mitigation*																		
03.d Risk Evaluation																		

HIPAA / CSF	**164.310(c)** Workstation Security	**164.310(d)(1)** Device & Media Controls	**164.310(d)(2)(i)** Disposal (R)	**164.310(d)(2)(ii)** Media Re-use (R)	**164.310(d)(2)(iii)** Accountability (A)	**164.310(d)(2)(iv)** Data Backup & Storage (A)	**164.312(a)(1)** Access Control	**164.312(a)(2)(i)** Unique User Identification (R)	**164.312(a)(2)(ii)** Emergency Access Procedure (R)	**164.312(a)(2)(iii)** Automatic Logoff (A)	**164.312(a)(2)(iv)** Encryption & Decryption (Stored) (A)	**164.312(b)** Audit Controls	**164.312(c)(1)** Integrity	**164.312(c)(2)** Mechanism to Authenticate ePHI (A)	**164.312(d)** Person or Entity Authentication	**164.312(e)(1)** Transmission Security	**164.312(e)(2)(i)** Integrity Controls (A)	**164.312(e)(2)(ii)** Encryption (Transmission) (A)
0.a InfoSec Mgmt Program																		
01.a Access Control Policy*		O					X											
01.b User Registration*								X	X						X			
01.c Privilege Management							X	X	X		O							
01.d User Password Management*																		
01.e Review of User Access Rights							X	X	X									
01.f Password Use*																		
01.g Unattended User Equipment	X									X								
01.h Clear Desk and Clear Screen Policy*	O	O				O	O			X			O					
01.i Policy on Use of Network Services*							X											
01.j User Auth. for Ext. Connections*								O							O			
01.k Equip Ident. in Networks								X							X			
01.l Remote Diagnostic & Config Port Protection	O						O											
01.m Segregation in Networks*																		
01.n Network Connection Control*																		
01.o Network Routing Control*																		
01.p Secure Log-on Procedures								O							O			
01.q User Identification and Authentication*								X	O						X			
01.r Password Mgmt System*																		
01.s Use of System Utilities							X	X	X		X	O						
01.t Session Time-out								O	O	X								
01.u Limitation of Connection Time								O	O									
01.v Information Access Restriction*							X	X	X		X							
01.w Sensitive System Isolation*																		
01.x Mobile Computing and Communications*					O		O											
01.y Teleworking*					O		O											
02.a Roles and Responsibilities*					O		O					O	O					
02.b Screening																		
02.c Terms and Conditions of Employment					X													
02.d Management Responsibilities*					O													
02.e InfoSec Awareness, Education, and Training*																		
02.f Disciplinary Process*																		
02.g Termination or Change Responsibilities																		
02.h Return of Assets																		
02.i Removal of Access Rights*								X	X									
03.a Risk Management Program Development																		
03.b Performing Risk Assessments*																		
03.c Risk Mitigation*																		
03.d Risk Evaluation																		

HIPAA / CSF	164.314(a)(1) Business Associate Contracts or Other Arrangements	164.314(a)(2)(i) Business Associate Contracts	164.314(a)(2)(ii) Other Arrangements	164.314(b)(1) Requirements for Group Health Plans	164.314(b)(2)(i) Implement Safeguards	164.314(b)(2)(ii) Ensure Adequate Separation	164.314(b)(2)(iii) Ensure Agents Safeguard	164.314(b)(2)(iv) Report Security Incidents	164.316(a) Policies and Procedures	164.316(b)(1) Documentation	164.316(b)(2)(i) Time Limit	164.316(b)(2)(ii) Availability	164.316(b)(2)(iii) Updates
0.a InfoSec Mgmt Program										X			X
01.a Access Control Policy*													
01.b User Registration*													
01.c Privilege Management													
01.d User Password Management*													
01.e Review of User Access Rights													
01.f Password Use*													
01.g Unattended User Equipment													
01.h Clear Desk and Clear Screen Policy*													
01.i Policy on Use of Network Services*													
01.j User Auth. for Ext. Connections*			O										
01.k Equip Ident. in Networks													
01.l Remote Diagnostic & Config Port Protection													
01.m Segregation in Networks*													
01.n Network Connection Control*													
01.o Network Routing Control*													
01.p Secure Log-on Procedures													
01.q User Identification and Authentication*													
01.r Password Mgmt System*													
01.s Use of System Utilities													
01.t Session Time-out													
01.u Limitation of Connection Time													
01.v Information Access Restriction*													
01.w Sensitive System Isolation*													
01.x Mobile Computing and Communications*	O	O	O										
01.y Teleworking*	O	O	O										
02.a Roles and Responsibilities*	O	O	O						O				
02.b Screening													
02.c Terms and Conditions of Employment	X	X	X										
02.d Management Responsibilities*	X	X	X										
02.e InfoSec Awareness, Education, and Training*													
02.f Disciplinary Process*													
02.g Termination or Change Responsibilities													
02.h Return of Assets													
02.i Removal of Access Rights*													
03.a Risk Management Program Development									X				
03.b Performing Risk Assessments*									X				
03.c Risk Mitigation*													
03.d Risk Evaluation													

HIPAA / CSF	164.308(a)(1)(i) Security Mgmt Process	164.308(a)(1)(ii)(A) Risk Analysis (R)	164.308(a)(1)(ii)(B) Risk Mgmt (R)	164.308(a)(1)(ii)(C) Sanction Policy (R)	164.308(a)(1)(ii)(D) Information System Activity Review (R)	164.308(a)(2) Assigned Security Responsibility	162.308(a)(3)(i) Workforce Security	164.308(a)(3)(ii)(A) Authorization and/ or Supervision (A)	164.308(a)(3)(ii)(B) Workforce Clearance Procedures (A)	164.308(a)(3)(ii)(C) Termination Procedures (A)	164.308(a)(4)(i) Information Access Management	164.308(a)(4)(ii)(A) Isolation Health Clearinghouse Functions (R)	164.308(a)(4)(ii)(B) Access Authorization	164.308(a)(4)(ii)(C) Access Establishment & Modificaiton (A)	164.308(a)(5)(i) Security Awareness Training	164.308(a)(5)(ii)(A) Security Reminders (A)	164.308(a)(5)(ii)(B) Protection from Malicious Software (A)	164.308(a)(5)(ii)(C) Log-in Monitoring (A)
04.a Information Security Policy Document*	O						O	O	O	O	O		O	O	O			
04.b Review of the InfoSec Policy*	O						O	O	O	O	O		O	O	O			
05.a Management Commitment to InfoSec*	O						O	X	X	X	O		O	O	O			
05.b InfoSec Coordination*	O		X				O	O	O	O	O		O	O	O			
05.c Allocation of InfoSec Responsibilities	O						O	O	O	O	O		O	O	O			
05.d Authorization Process for Info Assets and Facilities						X							O					
05.e Confidentiality Agreements								O	O				O					
05.f Contact with Authorities					O											O		
05.g Contact with Special Interest Groups															O	X		
05.h Independent Review of Information Security					X	O												
05.i Identification of Risks Related to External Parties*		O	O															
05.j Addressing Security When Dealing w/ Customers						O									O	O	O	
05.k Addressing Security in Third Party Agreements*								X	O				X					
06.a Identification of Applicable Legislation	O						O	O	O	O	O		O	O	O			
06.b Intellectual Property Rights																		
06.c Protection of Organizational Records								O					O	O				
06.d Data Protection and Privacy of Covered Info*																		
06.e Prevention of Misuse of Information Assets*				X	O			O	O		O		O					O
06.f Regulation of Cryptographic Controls																		
06.g Compliance with Security Policies and Stds*	O				X	X	O	O	O	O	O		O	O	O			
06.h Technical Compliance Checking					X	O												
06.i Information Systems Audit Controls			X														O	O
06.j Protection of Info Systems Audit Tools					O													
07.a Inventory of Assets*																		
07.b Ownership of Assets																		
07.c Acceptable Use of Assets*									O				O					
07.d Classification Guidelines		X	X															
07.e Information Labeling and Handling								O					O	O				
08.a Physical Security Perimeter								O										
08.b Physical Entry Controls*																		
08.c Securing Offices, Rooms, and Facilities																		
08.d Protecting Against External and Env. Threats*																		
08.e Working in Secure Areas																		
08.f Public Access, Delivery, and Loading Areas																		
08.g Equipment Siting and Protection																		
08.h Supporting Utilities																		
08.i Cabling Security																		
08.j Equipment Maintenance*								X										
08.k Security of Equipment Off-Premises																		

HIPAA / CSF	164.308(a)(5)(ii)(D) Password Management (A)	164.308(a)(6)(i) Security Incident Procedures	164.308(a)(6)(ii) Response & Reporting (R)	164.308(a)(7)(i) Contingency Plan	164.308(a)(7)(ii)(A) Data Backup Plan (R)	164.308(a)(7)(ii)(B) Disaster Recovery Plan (R)	164.308(a)(7)(ii)(C) Emergency Mode Operation Plan (R)	164.308(a)(7)(ii)(D) Testing & Revisoin Procedures (A)	164.308(a)(7)(ii)(E) Application and Data Criticality Analysis (A)	164.308(a)(8) Evaluation	164.308(b)(1) Business Associate Contracts & Other Arrangements	164.308(b)(4) Written Contract (R)	164.310(a)(1) Facility Access Controls	164.310(a)(2)(i) Contingency Operations (A)	164.310(a)(2)(ii) Facility Security Plan (A)	164.310(a)(2)(iii) Access Control Validation Procedures (A)	164.310(a)(2)(iv) Maintenance Records (A)	164.310(b) Workstation Use
04.a Information Security Policy Document*		O		O						O			O		O	O	O	
04.b Review of the InfoSec Policy*		O		O						O			O		O	O	O	
05.a Management Commitment to InfoSec*		O		O						O			O		O	O	O	
05.b InfoSec Coordination*		O	O			O	O	O	O	O			O	O	X	O	O	
05.c Allocation of InfoSec Responsibilities		O		O		O	O	O	O	O	O	O	O	O	O	O	O	
05.d Authorization Process for Info Assets and Facilities										X								
05.e Confidentiality Agreements											O	O						O
05.f Contact with Authorities			O															
05.g Contact with Special Interest Groups																		
05.h Independent Review of Information Security										X								
05.i Identification of Risks Related to External Parties*										O	X	X						
05.j Addressing Security When Dealing w/ Customers											O	O						
05.k Addressing Security in Third Party Agreements*											X	O						
06.a Identification of Applicable Legislation		O		O						O			O		O	O	O	
06.b Intellectual Property Rights																		
06.c Protection of Organizational Records					O	O										O		
06.d Data Protection and Privacy of Covered Info*																		
06.e Prevention of Misuse of Information Assets*																		O
06.f Regulation of Cryptographic Controls	X																	
06.g Compliance with Security Policies and Stds*				O						X			O		O	O	O	
06.h Technical Compliance Checking										X								
06.i Information Systems Audit Controls															X			
06.j Protection of Info Systems Audit Tools																		
07.a Inventory of Assets*																		
07.b Ownership of Assets																		
07.c Acceptable Use of Assets*																		
07.d Classification Guidelines																O		
07.e Information Labeling and Handling																		X
08.a Physical Security Perimeter													X			X		X
08.b Physical Entry Controls*													X			X		X
08.c Securing Offices, Rooms, and Facilities													X			X		X
08.d Protecting Against External and Env. Threats*					O	O	O	O	O				X	O	X	X		
08.e Working in Secure Areas													O		O	X		
08.f Public Access, Delivery, and Loading Areas													O			O		O
08.g Equipment Siting and Protection													X		X	X		
08.h Supporting Utilities						O												
08.i Cabling Security													X					
08.j Equipment Maintenance*																	X	O
08.k Security of Equipment Off-Premises														X				

HIPAA / CSF	164.310(c) Workstation Security	164.310(d)(1) Device & Media Controls	164.310(d)(2)(i) Disposal (R)	164.310(d)(2)(ii) Media Re-use (R)	164.310(d)(2)(iii) Accountability (A)	164.310(d)(2)(iv) Data Backup & Storage (A)	164.312(a)(1) Access Control	164.312(a)(2)(i) Unique User Identification (R)	164.312(a)(2)(ii) Emergency Access Procedure (R)	164.312(a)(2)(iii) Automatic Logoff (A)	164.312(a)(2)(iv) Encryption & Decryption (Stored) (A)	164.312(b) Audit Controls	164.312(c)(1) Integrity	164.312(c)(2) Mechanism to Authenticate ePHI (A)	164.312(d) Person or Entity Authentication	164.312(e)(1) Transmission Security	164.312(e)(2)(i) Integrity Controls (A)	164.312(e)(2)(ii) Encryption (Transmission) (A)
04.a Information Security Policy Document*		O					O					O	X					
04.b Review of the InfoSec Policy*		O					O					O	O					
05.a Management Commitment to InfoSec*		O					O					O	O					
05.b InfoSec Coordination*		O					O		O			O	O					
05.c Allocation of InfoSec Responsibilities		O					O		O			O	O					
05.d Authorization Process for Info Assets and Facilities																		
05.e Confidentiality Agreements					O													
05.f Contact with Authorities																		
05.g Contact with Special Interest Groups																		
05.h Independent Review of Information Security																		
05.i Identification of Risks Related to External Parties*																		
05.j Addressing Security When Dealing w/ Customers																		
05.k Addressing Security in Third Party Agreements*					O													
06.a Identification of Applicable Legislation		O					O	O	O			O	O					
06.b Intellectual Property Rights																		
06.c Protection of Organizational Records	O	O				O	O						O					
06.d Data Protection and Privacy of Covered Info*																		
06.e Prevention of Misuse of Information Assets*					O							O						
06.f Regulation of Cryptographic Controls											X							X
06.g Compliance with Security Policies and Stds*		O					O					O	O					
06.h Technical Compliance Checking																		
06.i Information Systems Audit Controls												X						
06.j Protection of Info Systems Audit Tools																		
07.a Inventory of Assets*		X			X													
07.b Ownership of Assets		X			X													
07.c Acceptable Use of Assets*					O													
07.d Classification Guidelines																		
07.e Information Labeling and Handling	X	X					O	O	O		O		O					
08.a Physical Security Perimeter	X																	
08.b Physical Entry Controls*	X																	
08.c Securing Offices, Rooms, and Facilities	X																	
08.d Protecting Against External and Env. Threats*	O								O									
08.e Working in Secure Areas	X																	
08.f Public Access, Delivery, and Loading Areas	O																	
08.g Equipment Siting and Protection	X																	
08.h Supporting Utilities																		
08.i Cabling Security	X																	
08.j Equipment Maintenance*																		
08.k Security of Equipment Off-Premises		X			X								X					

HIPAA / CSF	164.314(a)(1) Business Associate Contracts or Other Arrangements	164.314(a)(2)(i) Business Associate Contracts	164.314(a)(2)(ii) Other Arrangements	164.314(b)(1) Requirements for Group Health Plans	164.314(b)(2)(i) Implement Safeguards	164.314(b)(2)(ii) Ensure Adequate Separation	164.314(b)(2)(iii) Ensure Agents Safeguard	164.314(b)(2)(iv) Report Security Incidents	164.316(a) Policies and Procedures	164.316(b)(1) Documentation	164.316(b)(2)(i) Time Limit	164.316(b)(2)(ii) Availability	164.316(b)(2)(iii) Updates
04.a Information Security Policy Document*									O		X	X	
04.b Review of the InfoSec Policy*									X				
05.a Management Commitment to InfoSec*									X				
05.b InfoSec Coordination*									X	X			X
05.c Allocation of InfoSec Responsibilities	O	O	O						O				
05.d Authorization Process for Info Assets and Facilities													
05.e Confidentiality Agreements	O	O	O										
05.f Contact with Authorities		O											
05.g Contact with Special Interest Groups													
05.h Independent Review of Information Security													
05.i Identification of Risks Related to External Parties*	O	O	X						O				
05.j Addressing Security When Dealing w/ Customers	O	O	O										
05.k Addressing Security in Third Party Agreements*	X	X	X	X	X	X	X	X					
06.a Identification of Applicable Legislation									O				
06.b Intellectual Property Rights													
06.c Protection of Organizational Records													
06.d Data Protection and Privacy of Covered Info*													
06.e Prevention of Misuse of Information Assets*	O	O	O										
06.f Regulation of Cryptographic Controls													
06.g Compliance with Security Policies and Stds*									O				
06.h Technical Compliance Checking													
06.i Information Systems Audit Controls									X	X			X
06.j Protection of Info Systems Audit Tools													
07.a Inventory of Assets*													
07.b Ownership of Assets													
07.c Acceptable Use of Assets*	O	O	O										
07.d Classification Guidelines													
07.e Information Labeling and Handling													
08.a Physical Security Perimeter													
08.b Physical Entry Controls*													
08.c Securing Offices, Rooms, and Facilities													
08.d Protecting Against External and Env. Threats*													
08.e Working in Secure Areas													
08.f Public Access, Delivery, and Loading Areas													
08.g Equipment Siting and Protection													
08.h Supporting Utilities													
08.i Cabling Security													
08.j Equipment Maintenance*													
08.k Security of Equipment Off-Premises													

HIPAA / CSF	164.308(a)(1)(i) Security Mgmt Process	164.308(a)(1)(ii)(A) Risk Analysis (R)	164.308(a)(1)(ii)(B) Risk Mgmt (R)	164.308(a)(1)(ii)(C) Sanction Policy (R)	164.308(a)(1)(ii)(D) Information System Activity Review (R)	164.308(a)(2) Assigned Security Responsibility	162.308(a)(3)(i) Workforce Security	164.308(a)(3)(ii)(A) Authorization and/ or Supervision (A)	164.308(a)(3)(ii)(B) Workforce Clearance Procedures (A)	164.308(a)(3)(ii)(C) Termination Procedures (A)	164.308(a)(4)(i) Information Access Management	164.308(a)(4)(ii)(A) Isolation Health Clearinghouse Functions (R)	164.308(a)(4)(ii)(B) Access Authorization	164.308(a)(4)(ii)(C) Access Establishment & Modificaiton (A)	164.308(a)(5)(i) Security Awareness Training	164.308(a)(5)(ii)(A) Security Reminders (A)	164.308(a)(5)(ii)(B) Protection from Malicious Software (A)	164.308(a)(5)(ii)(C) Log-in Monitoring (A)
08.l Secure Disposal or Re-Use of Equipment*																		
08.m Removal of Property																		
09.a Documented Operations Procedures	O						O	O	O	O	O		O	O	O			
09.b Change Management																		
09.c Segregation of Duties*							X				X	X						
09.d Separation of Development, Test, and Operational Environments																		
09.e Service Delivery*																		
09.f Monitoring and Review of Third Party Services*																		
09.g Managing Changes to Third Party Services*																		
09.h Capacity Management																		
09.i System Acceptance						O												
09.j Controls Against Malicious Code*															O	O	X	
09.k Controls Against Mobile Code																	X	
09.l Back-up																		
09.m Network Controls*								O					O	O				
09.n Security of Network Services																		
09.o Management of Removable Media*																		
09.p Disposal of Media*																		
09.q Information Handling Procedures*								X					O	O				
09.r Security of System Documentation								O					O	O				
09.s Information Exchange Policies and Procedures*								O	O				O	O				
09.t Exchange Agreements																		
09.u Physical Media in Transit																		
09.v Electronic Messaging																		
09.w Interconnected Business Info Systems																		
09.x Electronic Commerce Services								O					O	O				
09.y On-line Transactions								O					O	O				
09.z Publicly Available Information					O			O					O	O		O	O	
09.aa Audit Logging*																		X
09.ab Monitoring System Use*					X			X			X		X				X	X
09.ac Protection of Log Information*					O												O	
09.ad Administrator and Operator Logs																		X
09.ae Fault Logging					O			O			O		O					X
09.af Clock Synchronization*																		
10.a Security Requirements Analysis and Specification		O	O															
10.b Input Data Validation*																		
10.c Control of Internal Processing																		
10.d Message Integrity																		
10.e Output Data Validation																		

HIPAA / CSF	164.308(a)(5)(ii)(D) Password Management (A)	164.308(a)(6)(i) Security Incident Procedures	164.308(a)(6)(ii) Response & Reporting (R)	164.308(a)(7)(i) Contingency Plan	164.308(a)(7)(ii)(A) Data Backup Plan (R)	164.308(a)(7)(ii)(B) Disaster Recovery Plan (R)	164.308(a)(7)(ii)(C) Emergency Mode Operation Plan (R)	164.308(a)(7)(ii)(D) Testing & Revisoin Procedures (A)	164.308(a)(7)(ii)(E) Application and Data Criticality Analysis (A)	164.308(a)(8) Evaluation	164.308(b)(1) Business Associate Contracts & Other Arrangements	164.308(b)(4) Written Contract (R)	164.310(a)(1) Facility Access Controls	164.310(a)(2)(i) Contingency Operations (A)	164.310(a)(2)(ii) Facility Security Plan (A)	164.310(a)(2)(iii) Access Control Validation Procedures (A)	164.310(a)(2)(iv) Maintenance Records (A)	164.310(b) Workstation Use
08.l Secure Disposal or Re-Use of Equipment*																		
08.m Removal of Property																	O	
09.a Documented Operations Procedures		O		O									O		O	O	X	
09.b Change Management																		
09.c Segregation of Duties*																		
09.d Separation of Development, Test, and Operational Environments																		
09.e Service Delivery*											X	X						
09.f Monitoring and Review of Third Party Services*											X	X						
09.g Managing Changes to Third Party Services*											O	O						
09.h Capacity Management						O	O	O	O					O				
09.i System Acceptance										O								
09.j Controls Against Malicious Code*		O																O
09.k Controls Against Mobile Code																		
09.l Back-up					X	X												
09.m Network Controls*											O	O				O		O
09.n Security of Network Services											X	X						
09.o Management of Removable Media*																		O
09.p Disposal of Media*																		
09.q Information Handling Procedures*																O		X
09.r Security of System Documentation																O		O
09.s Information Exchange Policies and Procedures*											O	O				O		X
09.t Exchange Agreements											O	O						
09.u Physical Media in Transit																		
09.v Electronic Messaging																		
09.w Interconnected Business Info Systems											X	X						O
09.x Electronic Commerce Services	O															O		O
09.y On-line Transactions	O															O		O
09.z Publicly Available Information																O		O
09.aa Audit Logging*																		
09.ab Monitoring System Use*																O		
09.ac Protection of Log Information*																		
09.ad Administrator and Operator Logs																		
09.ae Fault Logging																		
09.af Clock Synchronization*																		
10.a Security Requirements Analysis and Specification									O									
10.b Input Data Validation*																		
10.c Control of Internal Processing																		
10.d Message Integrity																		
10.e Output Data Validation																		

HIPAA / CSF	164.310(c) Workstation Security	164.310(d)(1) Device & Media Controls	164.310(d)(2)(i) Disposal (R)	164.310(d)(2)(ii) Media Re-use (R)	164.310(d)(2)(iii) Accountability (A)	164.310(d)(2)(iv) Data Backup & Storage (A)	164.312(a)(1) Access Control	164.312(a)(2)(i) Unique User Identification (R)	164.312(a)(2)(ii) Emergency Access Procedure (R)	164.312(a)(2)(iii) Automatic Logoff (A)	164.312(a)(2)(iv) Encryption & Decryption (Stored) (A)	164.312(b) Audit Controls	164.312(c)(1) Integrity	164.312(c)(2) Mechanism to Authenticate ePHI (A)	164.312(d) Person or Entity Authentication	164.312(e)(1) Transmission Security	164.312(e)(2)(i) Integrity Controls (A)	164.312(e)(2)(ii) Encryption (Transmission) (A)
08.l Secure Disposal or Re-Use of Equipment*		X	X	X														
08.m Removal of Property		O			O								O					
09.a Documented Operations Procedures		O					O					O	O					
09.b Change Management																		
09.c Segregation of Duties*							X											
09.d Separation of Development, Test, and Operational Environments																		
09.e Service Delivery*																		
09.f Monitoring and Review of Third Party Services*																		
09.g Managing Changes to Third Party Services*																		
09.h Capacity Management									O			X						
09.i System Acceptance																		
09.j Controls Against Malicious Code*													O	O			O	
09.k Controls Against Mobile Code																		
09.l Back-up						X							X					
09.m Network Controls*							O	X	O		O		X	X	X	X	X	X
09.n Security of Network Services																		
09.o Management of Removable Media*	X	X	O	O	X	X							X					
09.p Disposal of Media*		X	X	X														
09.q Information Handling Procedures*	X	X					O	O	O		O		X					
09.r Security of System Documentation	O	O				O	O	O	O		O							
09.s Information Exchange Policies and Procedures*					O		O	O	O		O		O	O		O	O	O
09.t Exchange Agreements																		
09.u Physical Media in Transit		X			X								X					
09.v Electronic Messaging													X	X		X	X	X
09.w Interconnected Business Info Systems																		
09.x Electronic Commerce Services							O	O	O		O		X	X	O	X	X	X
09.y On-line Transactions							O	O	O		O		O	O	O	O	O	O
09.z Publicly Available Information							O	O	O		O		O	O			O	
09.aa Audit Logging*												X						
09.ab Monitoring System Use*												X	O	O			O	
09.ac Protection of Log Information*												O						
09.ad Administrator and Operator Logs												X						
09.ae Fault Logging												X						
09.af Clock Synchronization*																		
10.a Security Requirements Analysis and Specification																		
10.b Input Data Validation*																		
10.c Control of Internal Processing													X	X			X	
10.d Message Integrity													X	X			X	
10.e Output Data Validation																		

HIPAA / CSF	**164.314(a)(1)** Business Associate Contracts or Other Arrangements	**164.314(a)(2)(i)** Business Associate Contracts	**164.314(a)(2)(ii)** Other Arrangements	**164.314(b)(1)** Requirements for Group Health Plans	**164.314(b)(2)(i)** Implement Safeguards	**164.314(b)(2)(ii)** Ensure Adequate Separation	**164.314(b)(2)(iii)** Ensure Agents Safeguard	**164.314(b)(2)(iv)** Report Security Incidents	**164.316(a)** Policies and Procedures	**164.316(b)(1)** Documentation	**164.316(b)(2)(i)** Time Limit	**164.316(b)(2)(ii)** Availability	**164.316(b)(2)(iii)** Updates
08.l Secure Disposal or Re-Use of Equipment*													
08.m Removal of Property													
09.a Documented Operations Procedures									O				
09.b Change Management													
09.c Segregation of Duties*													
09.d Separation of Development, Test, and Operational Environments													
09.e Service Delivery*	X	X	X										
09.f Monitoring and Review of Third Party Services*	X	X	X										
09.g Managing Changes to Third Party Services*	O	O	O										
09.h Capacity Management													
09.i System Acceptance		O											
09.j Controls Against Malicious Code*													
09.k Controls Against Mobile Code													
09.l Back-up													
09.m Network Controls*			O										
09.n Security of Network Services	X	X	X										
09.o Management of Removable Media*													
09.p Disposal of Media*													
09.q Information Handling Procedures*													
09.r Security of System Documentation													
09.s Information Exchange Policies and Procedures*	O	O	O										
09.t Exchange Agreements	O	O	O										
09.u Physical Media in Transit													
09.v Electronic Messaging													
09.w Interconnected Business Info Systems			X										
09.x Electronic Commerce Services													
09.y On-line Transactions													
09.z Publicly Available Information													
09.aa Audit Logging*													
09.ab Monitoring System Use*													
09.ac Protection of Log Information*													
09.ad Administrator and Operator Logs													
09.ae Fault Logging													
09.af Clock Synchronization*													
10.a Security Requirements Analysis and Specification		X											
10.b Input Data Validation*													
10.c Control of Internal Processing													
10.d Message Integrity													
10.e Output Data Validation													

CSF - HIPAA Cross-Reference Matrix v3

HIPAA / CSF	**164.308(a)(1)(i)** Security Mgmt Process	**164.308(a)(1)(ii)(A)** Risk Analysis (R)	**164.308(a)(1)(ii)(B)** Risk Mgmt (R)	**164.308(a)(1)(ii)(C)** Sanction Policy (R)	**164.308(a)(1)(ii)(D)** Information System Activity Review (R)	**164.308(a)(2)** Assigned Security Responsibility	**162.308(a)(3)(i)** Workforce Security	**164.308(a)(3)(ii)(A)** Authorization and/ or Supervision (A)	**164.308(a)(3)(ii)(B)** Workforce Clearance Procedures (A)	**164.308(a)(3)(ii)(C)** Termination Procedures (A)	**164.308(a)(4)(i)** Information Access Management	**164.308(a)(4)(ii)(A)** Isolation Health Clearinghouse Functions (R)	**164.308(a)(4)(ii)(B)** Access Authorization	**164.308(a)(4)(ii)(C)** Access Establishment & Modificaiton (A)	**164.308(a)(5)(i)** Security Awareness Training	**164.308(a)(5)(ii)(A)** Security Reminders (A)	**164.308(a)(5)(ii)(B)** Protection from Malicious Software (A)	**164.308(a)(5)(ii)(C)** Log-in Monitoring (A)
10.f Policy on the Use of Cryptographic Controls*																		
10.g Key Management*																		
10.h Control of Operational Software*																		
10.i Protection of System Test Data																		
10.j Access Control to Program Source Code							O	O			O	O						
10.k Change Control Procedures								O					O					
10.l Outsourced Software Development*																		
10.m Control of Technical Vulnerabilities*		O	O		O											O		
11.a Reporting Information Security Events*					X			O			O		O					O
11.b Reporting Security Weaknesses					O	O										O		
11.c Responsibilities and Procedures*					X													
11.d Learning from InfoSec Incidents					X													
11.e Collection of Evidence					O													
12.a Including InfoSec in the BC Mgmt Process																		
12.b Business Continuity and Risk Assessment	O	O	O															
12.c Develop/Implement BC Plans incl InfoSec*																		
12.d Business Continuity Planning Framework																		
12.e Testing, Maintaining & Re-Assessing BC Plans																		

X - Primary, direct relationship
O - Secondary , supporting relationship
***** Required for HITRUST 2012 Certification
(A) Addressable Implementation Specification
(R) Required Implementatoin Specification

CSF - HIPAA Cross-Reference Matrix v3

HIPAA / CSF	**164.308(a)(5)(ii)(D)** Password Management (A)	**164.308(a)(6)(i)** Security Incident Procedures	**164.308(a)(6)(ii)** Response & Reporting (R)	**164.308(a)(7)(i)** Contingency Plan	**164.308(a)(7)(ii)(A)** Data Backup Plan (R)	**164.308(a)(7)(ii)(B)** Disaster Recovery Plan (R)	**164.308(a)(7)(ii)(C)** Emergency Mode Operation Plan (R)	**164.308(a)(7)(ii)(D)** Testing & Revisoin Procedures (A)	**164.308(a)(7)(ii)(E)** Application and Data Criticality Analysis (A)	**164.308(a)(8)** Evaluation	**164.308(b)(1)** Business Associate Contracts & Other Arrangements	**164.308(b)(4)** Written Contract (R)	**164.310(a)(1)** Facility Access Controls	**164.310(a)(2)(i)** Contingency Operations (A)	**164.310(a)(2)(ii)** Facility Security Plan (A)	**164.310(a)(2)(iii)** Access Control Validation Procedures (A)	**164.310(a)(2)(iv)** Maintenance Records (A)	**164.310(b)** Workstation Use
10.f Policy on the Use of Cryptographic Controls*																		
10.g Key Management*																		
10.h Control of Operational Software*																		
10.i Protection of System Test Data																		
10.j Access Control to Program Source Code																		
10.k Change Control Procedures																		O
10.l Outsourced Software Development*											O	O						
10.m Control of Technical Vulnerabilities*										O								
11.a Reporting Information Security Events*		X	X															
11.b Reporting Security Weaknesses										O								
11.c Responsibilities and Procedures*		X	X															
11.d Learning from InfoSec Incidents			X															
11.e Collection of Evidence			X															
12.a Including InfoSec in the BC Mgmt Process				O		X	X	X	X					X				
12.b Business Continuity and Risk Assessment						O	O	O	O					O				
12.c Develop/Implement BC Plans incl InfoSec*				X	X	X	X	X	X					X				
12.d Business Continuity Planning Framework						X	X	O	X					X				
12.e Testing, Maintaining & Re-Assessing BC Plans						X	X	X	X					X				

X - Primary, direct relationship
O - Secondary , supporting relationship
***** Required for HITRUST 2012 Certification
(A) Addressable Implementation Specification
(R) Required Implementatoin Specification

CSF - HIPAA Cross-Reference Matrix v3

HIPAA / CSF	**164.310(c)** Workstation Security	**164.310(d)(1)** Device & Media Controls	**164.310(d)(2)(i)** Disposal (R)	**164.310(d)(2)(ii)** Media Re-use (R)	**164.310(d)(2)(iii)** Accountability (A)	**164.310(d)(2)(iv)** Data Backup & Storage (A)	**164.312(a)(1)** Access Control	**164.312(a)(2)(i)** Unique User Identification (R)	**164.312(a)(2)(ii)** Emergency Access Procedure (R)	**164.312(a)(2)(iii)** Automatic Logoff (A)	**164.312(a)(2)(iv)** Encryption & Decryption (Stored) (A)	**164.312(b)** Audit Controls	**164.312(c)(1)** Integrity	**164.312(c)(2)** Mechanism to Authenticate ePHI (A)	**164.312(d)** Person or Entity Authentication	**164.312(e)(1)** Transmission Security	**164.312(e)(2)(i)** Integrity Controls (A)	**164.312(e)(2)(ii)** Encryption (Transmission) (A)
10.f Policy on the Use of Cryptographic Controls*		O									X							X
10.g Key Management*																		X
10.h Control of Operational Software*													O	O			O	
10.i Protection of System Test Data																		
10.j Access Control to Program Source Code							O											
10.k Change Control Procedures																		
10.l Outsourced Software Development*																		
10.m Control of Technical Vulnerabilities*																		
11.a Reporting Information Security Events*												O						
11.b Reporting Security Weaknesses																		
11.c Responsibilities and Procedures*																		
11.d Learning from InfoSec Incidents																		
11.e Collection of Evidence												O						
12.a Including InfoSec in the BC Mgmt Process									X									
12.b Business Continuity and Risk Assessment									O									
12.c Develop/Implement BC Plans incl InfoSec*						X			X				X					
12.d Business Continuity Planning Framework									X									
12.e Testing, Maintaining & Re-Assessing BC Plans									X									

X - Primary, direct relationship
O - Secondary , supporting relationship
***** Required for HITRUST 2012 Certification
(A) Addressable Implementation Specification
(R) Required Implementatoin Specification

HIPAA / CSF	**164.314(a)(1)** Business Associate Contracts or Other Arrangements	**164.314(a)(2)(i)** Business Associate Contracts	**164.314(a)(2)(ii)** Other Arrangements	**164.314(b)(1)** Requirements for Group Health Plans	**164.314(b)(2)(i)** Implement Safeguards	**164.314(b)(2)(ii)** Ensure Adequate Separation	**164.314(b)(2)(iii)** Ensure Agents Safeguard	**164.314(b)(2)(iv)** Report Security Incidents	**164.316(a)** Policies and Procedures	**164.316(b)(1)** Documentation	**164.316(b)(2)(i)** Time Limit	**164.316(b)(2)(ii)** Availability	**164.316(b)(2)(iii)** Updates
10.f Policy on the Use of Cryptographic Controls*													
10.g Key Management*													
10.h Control of Operational Software*													
10.i Protection of System Test Data													
10.j Access Control to Program Source Code													
10.k Change Control Procedures													
10.l Outsourced Software Development*	O	O	O										
10.m Control of Technical Vulnerabilities*									O				
11.a Reporting Information Security Events*		X											
11.b Reporting Security Weaknesses													
11.c Responsibilities and Procedures*													
11.d Learning from InfoSec Incidents													
11.e Collection of Evidence													
12.a Including InfoSec in the BC Mgmt Process													
12.b Business Continuity and Risk Assessment									O				
12.c Develop/Implement BC Plans incl InfoSec*													
12.d Business Continuity Planning Framework													
12.e Testing, Maintaining & Re-Assessing BC Plans													

X - Primary, direct relationship
O - Secondary , supporting relationship
***** Required for HITRUST 2012 Certification
(A) Addressable Implementation Specification
(R) Required Implementatoin Specification